FORTINET

February 2023

Global Threat Landscape Report

A Semiannual Report by FortiGuard Labs

TABLE OF CONTENTS

Executive Summary

Cyber threats aren't going anywhere. And let's face it, cybercrime is one of the most–if not the most–profitable illegal industries in the world. With their own brand of Key Performance Indicators tied to return on investment, threat actors are more methodical and becoming more and more innovative in their tactics, including reviving old methods that have long been forgotten. After all, producers love a good remake of an old classic if it can make new money.

FortiGuard Labs experts leverage Fortinet's large global footprint to continually monitor the threat landscape and the major geopolitical events that influence it. This report presents findings and insights from six months of intense research, with recommendations for leaders and practitioners to better prepare and protect your organization. Read the latest report for a comprehensive view of the most significant outbreaks in 2022. And for real-time updates on the threat landscape, please register for our Outbreak Alerts.

Key highlights of the second half of 2022:

Don't count out the old

We saw the resurgence of familiar names in the malware, wiper, and botnet space–including Emotet and GandCrab, to name a few, in addition to code reuse (old code being recompiled into new variants)–a reminder that old malware and threats never die. They simply crawl back into the shadows waiting patiently for another turn.

Ransomware and Wipers

Volume is still growing: There's been a 16% increase in both ransomware and wipers. However, when we look at a quarterly breakdown, we see that wiper volume increased an astonishing 53% between Q3 and Q4 of 2022.

Introducing "The Red Zone"

Less than 1% of the total observed vulnerabilities discovered in an enterprise-size organization were on endpoints and actively under attack. This insight gives CISOs a clear view of the "Red Zone" or active attack surface.

Raspberry.Robin: a new bot with an old trick

1 in 84 organizations that detected botnet activity were impacted by this new botnet that only entered the bot scene in September.

Exchange becomes a post-exploitation hotpot

Hardening activities on Exchange servers have thwarted much initial access targeting. Adversary familiarity with associated services means Exchange servers have become a hotbed for post-exploitation activity.

ATT&CK

Keep an eye out for Pre-ATT&CK

Adversaries are dedicating more resources to their attacks' Recon and Weaponization phase. As this approach becomes more 'de-facto' among threat actors, cyber defenders must keep up using intelligence gathered from these phases.

Reconnaissance and Resource Development

Seeing what attackers do before they show up at an organization's digital doorstep is out of scope for the telemetry available to most organizations. However, there are several tools businesses can use to stay on top of the tactics, techniques, and trends (TTPs) that can highlight the methods a criminal uses to penetrate the organization's perimeter.

The threat landscape is also constantly shifting in terms of Reconnaissance and Resource Development, making it imperative for organizations to stay ahead of potential security threats. This requires a thorough understanding of cyber attackers' latest trends and techniques, which can help organizations better protect their assets and data.

In this section of the report, we look at what we can see in these phases—which generally occur in Dark and Deep Web forums, Telegram groups, and other avenues of information dissemination where Threat Actors discuss vulnerabilities, defenses, and malicious payloads. We actively monitor Telegram Groups that constantly advertise PoC (Proof of Concept) exploits and new malicious payloads. The graph below shows the number of times a threat actor has delivered information through this channel and the reliability of that data.

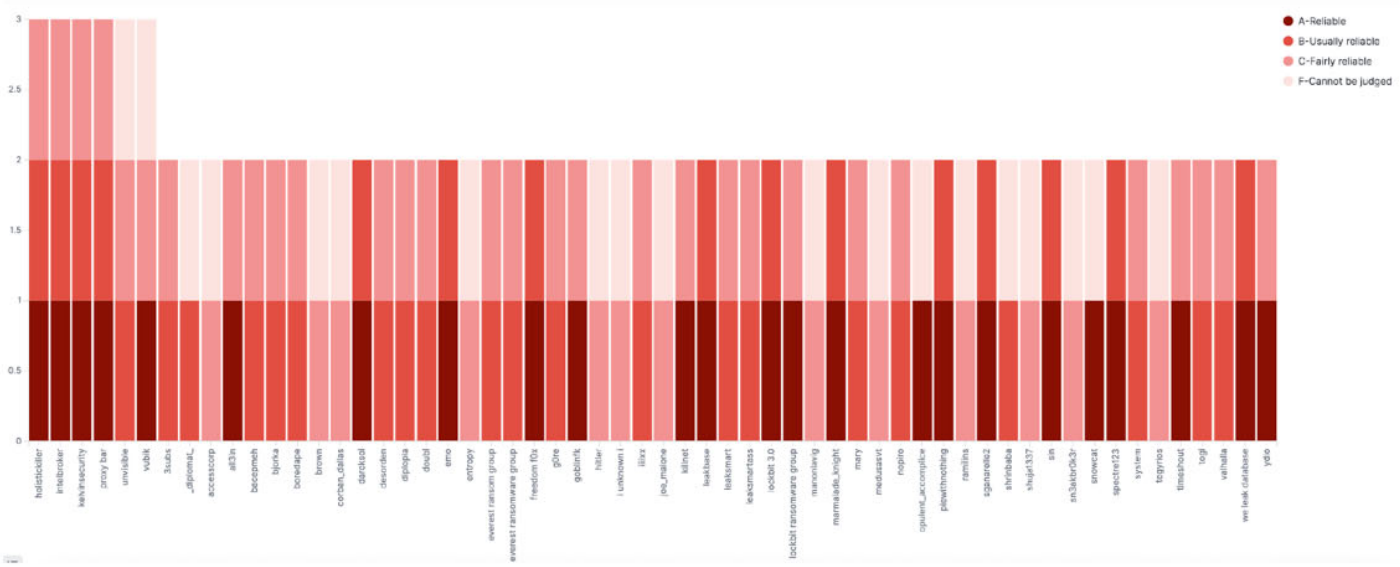

Figure 1 - Activity of actors and the reliability of their information

Telegram has seen a surge in popularity as a platform for anonymous communication, becoming a hub for cybercriminal activities. Over the past few years, this messaging service has become a preferred choice for threat actors engaged in fraudulent activities and the sale of stolen data. The following are key factors that make Telegram a favored alternative to the Darknet:

- The ability to send and receive large data files directly through the app, including text and zip files.
- A user-friendly setup requiring only a mobile phone number, which is reportedly hidden from other users and enables communication among tens of thousands of users.
- Greater accessibility and functionality and a lower risk of being tracked by law enforcement than dark web forums.
- Encrypted messaging and anonymity provide a high level of privacy and security for users.

By providing these features, Telegram has become popular for those seeking secure and anonymous communication. Preliminary activities observed on Telegram channels include:

- Sharing and advertising stolen data
- Various access to compromised infrastructure
- Exploits for zero-days and vulnerabilities
- DDoS and website defacements activities
- Distribution of hacking tools and stealer logs

The information in this report can be used to keep an eye on these channels to determine if they are putting out PoC exploits that might increase your risk of a particular vulnerability being exploited. The reliability of the information is measured, for instance, by whether a PoC exploit is working or not or if it just needs a 'tweak' to work–as was the case in the late 1990s when PoC exploits were shared on IRC channels and hackers would have to understand a bit of what was going on to replicate the attack.

By looking at the activity of ransomware groups on the Deep Web, we can determine how many victims each ransomware has accumulated. The chart below represents the Ransomware groups that have been active in this quarter, along with a respective count of their victims:

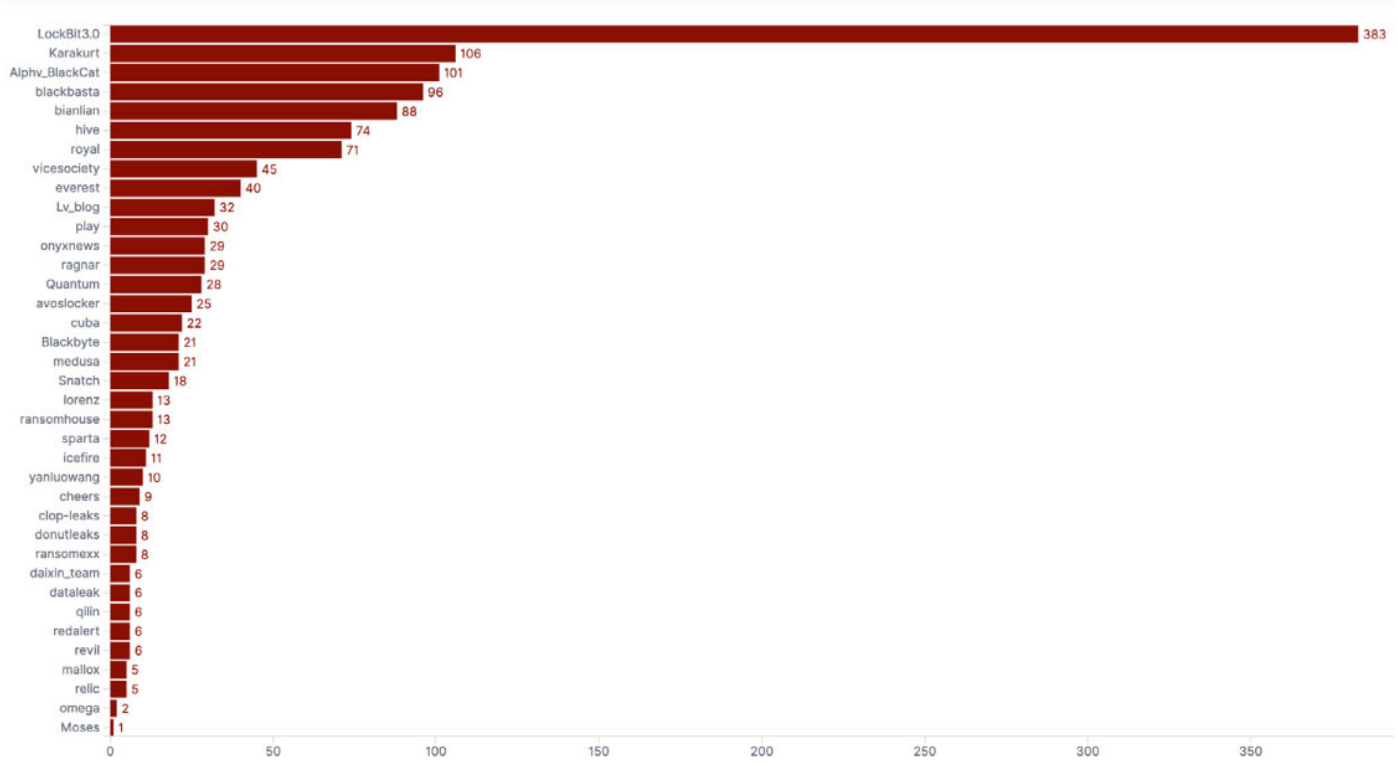

Figure 2 - Number of ransomware Victims advertised in the Deep Web

The graphic below shows how likely a vulnerability is to be mass exploited based on the chatter in these underground forums:

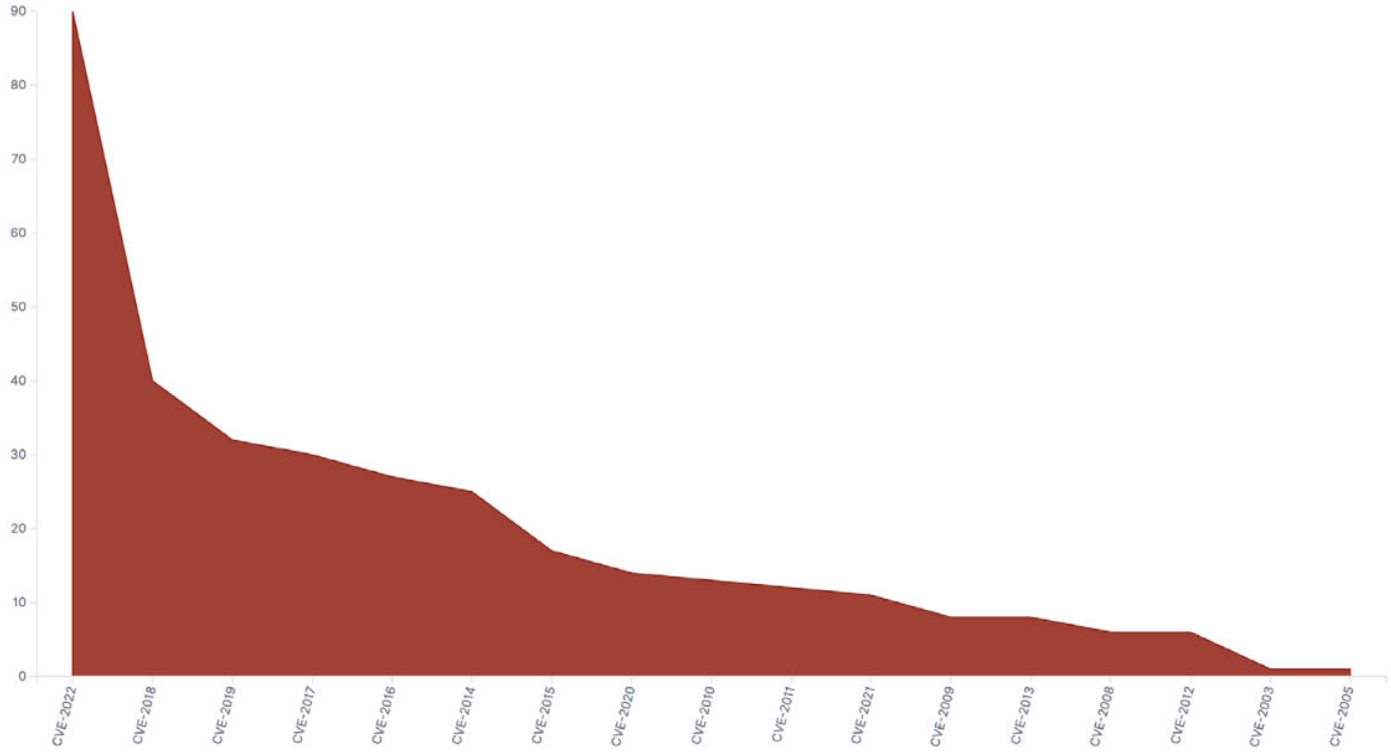

Figure 3 - Vulnerability Chatter on the Deep Web by Year of Disclosure

For obvious reasons, newer vulnerabilities draw more attention, partly because they are prone to be found in more systems due to targets having less time to implement patches. When new vulnerabilities have PoC exploits, some of the chatter also revolves around developing, testing, and fine-tuning these exploits to work on the different versions of the operating systems in which the vulnerability was found.

Being proactive in stopping adversaries as early as possible comes with many benefits. The impact of a potential attack or breach is significantly lower or can even be eliminated in some cases using the following best practices:

- Gathering information using a digital risk protection solution.
- Developing better insights and control over your external attack surface, including high-quality intelligence on adversaries to protect your organization and its brand.
- Testing tools and structured testing methods against the latest TTPs hacker use.
- Incorporating deception technology to deter criminals away from actual assets, instead drawing their attention to a decoy or trap to better understand their attack methods against your organization. This can help you improve security controls accordingly.

Initial Access: Technique Highlights

The use of valid credentials was increasingly prevalent among IR engagements investigated by the FortiGuard IR team in 2022. They account for ~44% of initial access methods, as shown in Figure 4 below.

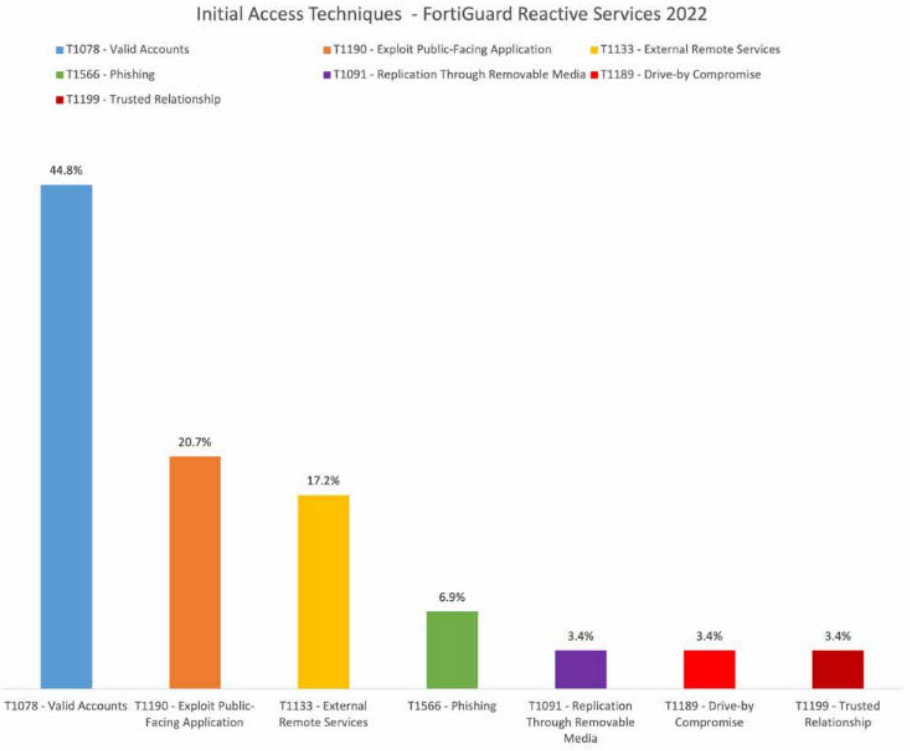

Figure 4 - Initial Access techniques observed as part of FortiGuard IR investigations

Data on using valid credentials for initial access is derived from investigations where the earliest adversary activity that could be linked to an intrusion is a logon using legitimate credentials. This can occur for several reasons, but the most likely are:

- The adversary collected credentials through an earlier activity that could not be linked to an intrusion, e.g., a credential harvesting campaign prior to the incident that went unreported.
- The adversary purchased credentials from an access broker who gained victim credentials through a previous compromise.

In most of these situations, there were vulnerable services on network devices (e.g., the management interface for a network device) or endpoints (e.g., a remote desktop protocol [RDP] connection to the internet) that were present in the victim's environment for extended periods prior to the attack. Such weaknesses in the network attack surface likely contributed to valid account details being accessed by the adversary, with initial access gained using T1133 – External Remote Services or T1190 – Exploit Public-Facing Application exploits.

Using valid accounts gives adversaries an advantage as they bypass opportunities for early kill chain detection that can often more easily identify an attack. Using valid accounts is also a defense evasion technique, as it can be difficult to differentiate between using legitimate credentials and a threat actor's misuse of legitimate credentials. This issue is exasperated when legitimate and adversary activities with the same valid account overlap.

The traditional view of a cyber intrusion is that a threat actor gains access to an environment by exploiting a vulnerability somewhere in the attack surface, drops some form of malware, progresses through the kill chain sequentially, and then performs their actions on objectives. However, when valid credentials are available, many detections that a SOC team may

rely on to identify malicious behavior are sidestepped. In one ransomware investigation, for example, the adversary used valid accounts to move through an environment and deploy a BitLocker-based ransomware script through an RDP. In this incident, the time involved from initial access to the deployment of ransomware was four hours. The threat actor only used valid methods of moving laterally through the network by exploiting legitimate credentials, then delivered ransomware without using any 'malware.'

A MITRE ATT&CK overlay for TTPs employed as part of this intrusion is shown below in Figure 5.

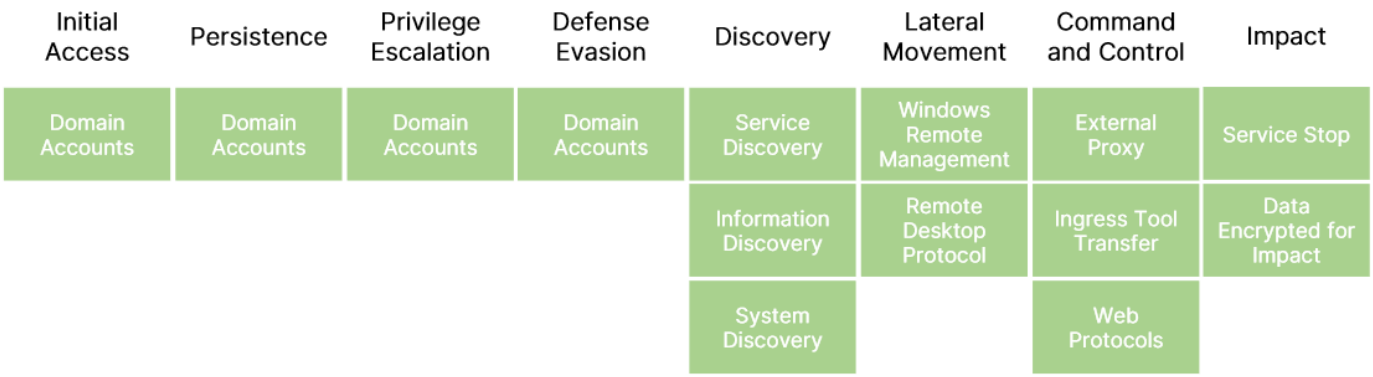

Figure 5 - MITRE ATT&CK Techniques employed as part of intrusion that lasted four hours between initial access and ransomware deployment.

TTP Heatmaps

It's not all terrible news if you find yourself with malware on one of your systems. Defenders can still contain the compromise if they can detect and respond. Let's look at the graph below to examine what we have seen with some samples to determine if we can spot criminals' most popular tactics and techniques.

This data is gathered from samples collected in the wild for each region and industry. We then use our sample tracker system to see if we already have that specific sample. If so, we run it through a sandbox to get its dynamic execution behavior, revealing its MITRE ATT&CK TTPs.

Different regions often have wildly different ratios when comparing how many samples we have for that area. This means that if a specific statistic for a region seems odd, it may be due to a lack of data from that particular location. This is often due to one region being more heavily attacked by an exploit not seen in other areas. It can also be due to new hashes that are nowhere to be found.

Keep in mind that this graphic only captures the most active techniques. Less used methods are omitted for simplicity's sake.

If you want to explore more, please sign-up for our free tool: **FortiGuard Threat Intel Insider**, via this link. This excellent threat intel tool lets you explore the TTPs and mitigation options for your region and industry per quarter. Historical threat data and executive summaries make this tool even more useful.

MITRE Sightings Ecosystem project

Fortinet is a Research Partner with MITRE Engenuity Center for Threat Informed Defense. In 2022 we led the MITRE Sightings Ecosystem project, which is now published. This ecosystem connects reporting of TTPs and these heatmaps are an example of our implementation.

Read more about this project where FortiGuard Labs is playing a leading research role.

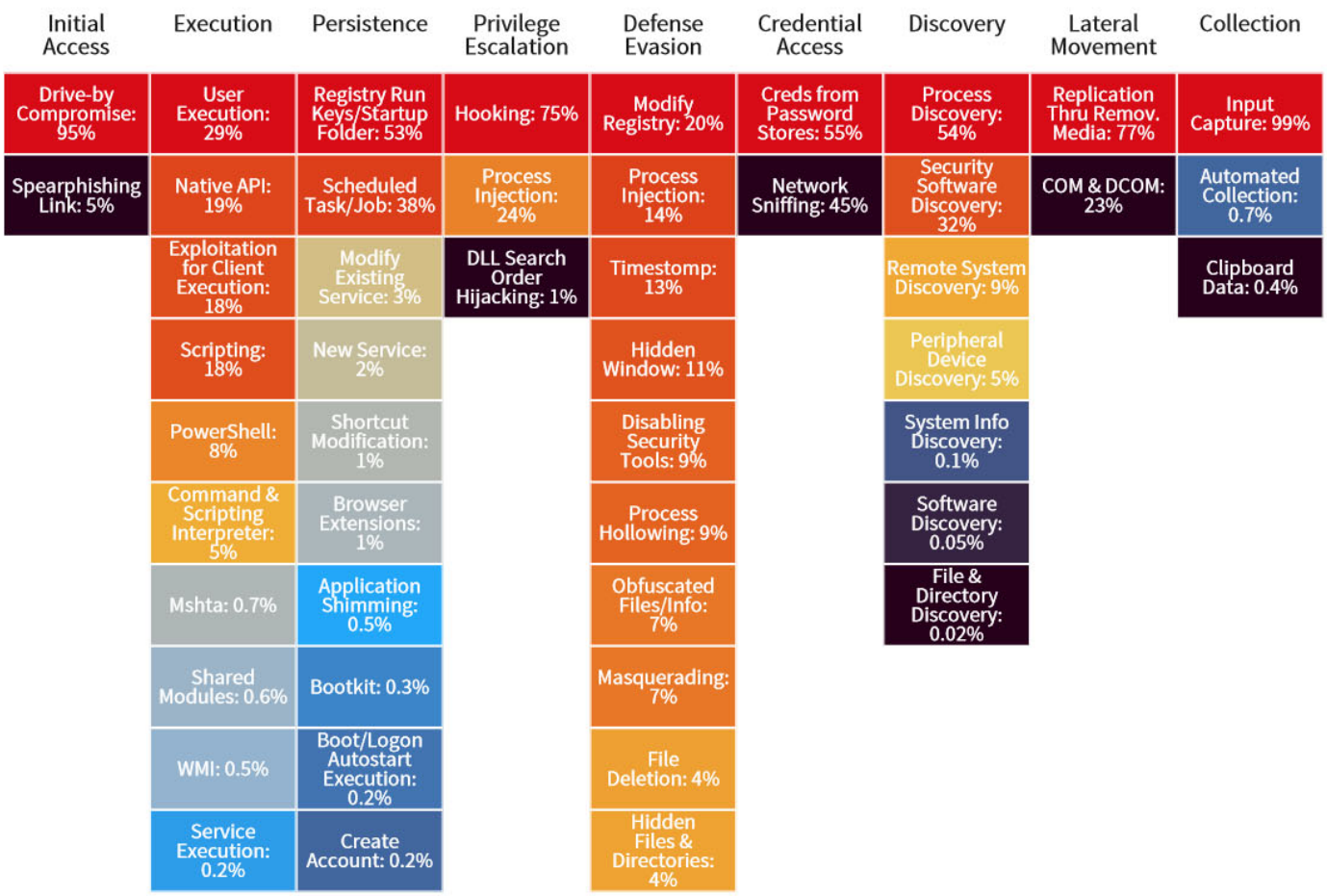

Figure 6 - Techniques in FortiSandbox Cloud data by tactic

In H2 2022, Drive-by Compromise was the most popular tactic used by criminals to gain access to an organization's systems, as indicated using Sandbox detonation. According to MITRE, adversaries gain access to their victims' systems when a victim is browsing the Internet. Looking at the ransomware and wipers trends in this chart, it makes sense that the initial access technique is being used, especially with some revived malware. We have also recently seen a surge in malware delivered through malicious JavaScript and ads. Several campaigns were seen exploiting this. Let's take a closer look to see what this change looks like across all regions and TTPs.

		Africa	Asia	Europe	N. America	Oceania	S. America
Initial Access	Drive-by Compromise	100%	92%	94%	100%	100%	100%
	Spearphishing Link	0%	8%	6%	0%	0%	0%
Execution	User Execution	29%	33%	32%	23%	30%	25%
	Native API	21%	17%	20%	19%	28%	18%
	Exploitation for Client Execution	15%	21%	10%	32%	9%	32%
	Scripting	21%	12%	24%	13%	18%	8%
	PowerShell	7%	8%	9%	8%	13%	9%
	Command & Scripting Interpreter	5%	6%	4%	4%	2%	5%
	Mshta	0.8%	1%	0.7%	0.9%	0.4%	0.1%
	Shared Modules	0.1%	0.6%	0.2%	0.7%	0.03%	2%
	WMI	0.4%	0.2%	0.9%	0.1%	0.07%	0.5%
	Service Execution	0.1%	0.2%	0.3%	0.04%	0.007%	0.2%
Persistence	Registry Run Keys/Startup Folder	50%	44%	63%	48%	38%	48%
	Scheduled Task/Job	43%	47%	26%	47%	58%	45%
	Modify Existing Service	2%	3%	4%	0.8%	1%	0.7%
	New Service	1%	3%	3%	0.4%	0.5%	0.5%
	Shortcut Modification	2%	2%	1%	1%	0.6%	2%
	Browser Extensions	0.7%	1%	0.7%	2%	1%	4%
	Application Shimming	0.4%	0.3%	0.9%	0.03%	0.01%	0%
	Bootkit	0.3%	0.02%	0.6%	0.1%	0%	0.01%
	Boot/Logon Autostart Execution	0.1%	0.05%	0.4%	0.4%	0%	0%
	Create Account	0.2%	0.1%	0.3%	0.2%	0.2%	0.1%
	Pre-OS Boot	0%	0%	0%	0%	0%	0%
Privilege Escalation	Hooking	74%	74%	81%	71%	75%	70%
	Process Injection	25%	25%	18%	29%	25%	28%
	DLL Search Order Hijacking	0.6%	1%	1%	0.2%	0.05%	1%
Defense Evasion	Modify Registry	19%	23%	16%	24%	14%	23%
	Process Injection	15%	14%	12%	14%	17%	15%
	Timestomp	12%	13%	14%	11%	14%	12%
	Hidden Window	10%	9%	14%	9%	10%	9%
	Disabling Security Tools	10%	10%	8%	10%	12%	11%
	Process Hollowing	10%	8%	9%	9%	11%	10%
	Obfuscated Files/Info	7%	8%	7%	6%	4%	5%
	Masquerading	6%	7%	7%	6%	9%	6%
	File Deletion	4%	3%	5%	3%	3%	3%
	Hidden Files & Directories	4%	4%	3%	4%	4%	4%
Credential Access	Creds from Password Stores	60%	75%	37%	80%	79%	69%
	Network Sniffing	40%	25%	63%	20%	21%	31%
Discovery	Process Discovery	55%	55%	46%	63%	58%	62%
	Security Software Discovery	34%	30%	40%	21%	28%	24%
	Remote System Discovery	8%	10%	9%	9%	11%	9%
	Peripheral Device Discovery	3%	4%	5%	7%	3%	6%
	System Info Discovery	0.09%	0.003%	0.3%	0.005%	0.02%	0.02%
	Software Discovery	0.04%	0.02%	0.1%	0%	0%	0%
	File & Directory Discovery	0%	0.01%	0.04%	0%	0.02%	0%
Lateral Movement	Replication Thru Remov. Media	69%	64%	85%	80%	88%	80%
	COM & DCOM	31%	36%	15%	20%	12%	20%
Collection	Input Capture	99%	100%	98%	100%	100%	100%
	Automated Collection	0.7%	0%	1%	0.1%	0%	0%
	Clipboard Data	0.3%	0.1%	0.8%	0%	0%	0%

Figure 7 - Techniques in FortiSandbox Cloud data by tactic and region

Across all regions, the initial access point is almost always Drive-by Compromise. There are some regional variations when we get into the different techniques used. For example, User Execution is the top tactic for nearly all regions except for North America and South America–where the top tactic is Exploitation for Client Execution. In this tactic, malicious users exploit vulnerabilities in various client applications to execute their code. This makes sense since it is also the perfect tactic to follow an access point attack driven by Drive-by Compromise.

Vulnerabilities

Attack Surface

The Cybersecurity & Infrastructure Security Agency's (CISA) Known Exploit Vulnerability (KEV) data is the authoritative source for exploits found in the wild. Based on our Incident Response engagements, T1190 Exploit Public-Facing Applications was the second most common way for actors to gain initial access to the network. Examining exploits shows us what criminals are interested in and are generally focused on, so keeping our fingers on the pulse here is essential.

Proactively monitoring the threat landscape – FortiGuard Labs has analysts around the globe proactively monitoring the threat intel landscape for newly disclosed vulnerabilities 24/7. Our research team, for example, has discovered 995 zero-day vulnerabilities. These research efforts ensure that customers are protected in real-time or close to real-time. Analysts are in the "trenches" where they are continuously monitoring publicly available resources for newly found and disclosed vulnerabilities so available proof of concept code and guidance can be reviewed for signature creation feasibility. During this time, internal teams carefully examine all signatures to ensure they pass stringent QA tests, protecting FortiGuard Labs customers.

The Proof is in the Pudding

Based on our IR engagements, T1190 Exploit Public-Facing Applications were the second-most popular way actors gained access to the network (Initial Access).

Learn more and stay protected.

Because Fortinet is part of the Microsoft Active Protections Program (MAPP), we receive guidance on high-severity vulnerabilities before Patch Tuesday from Microsoft and Adobe. This provides customers with an additional layer of protection. In addition, Fortinet is a member of the Cyber Threat Alliance (CTA). Through this partnership, blogs reporting threat discoveries and analyses from partners and members are shared before release to ensure all members have coverage before they are published.

To find these exploits, we look at IPS activity captured by the FortiGuard Intrusion Prevention System (IPS) Security Service sensors and unknown threats analyzed by our AI-Powered Inline Sandbox technology running on our Fabric (endpoint, network, and cloud) solutions. In the parlance of the popular MITRE ATT&CK framework, these detections often correspond to the Reconnaissance, Resource Development, and Initial Access techniques.

In addition to looking at IPS activity, we're building on what we introduced in the last report–endpoint vulnerabilities. Think of it this way, if we view endpoint vulnerabilities as the "Open Attack Surface," we can call the point where they overlap with IPS activity the "Active Attack Surface."

So, what did the overall CVE attack surface look like in the second half of 2022?

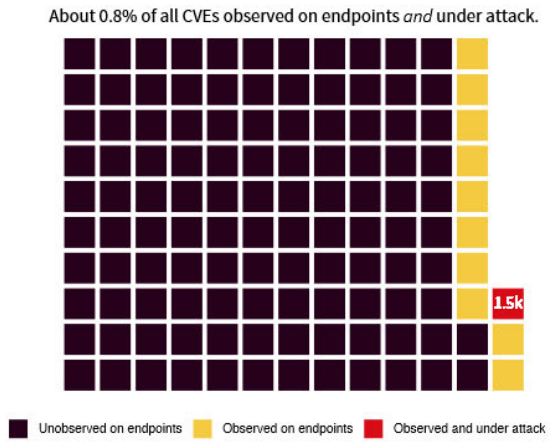

Figure 8 - All CVEs arranged by their presence on endpoints and in IPS telemetry

We can see clearly that the "active attack surface" is small. In fact, according to our FortiClient Vulnerability data, less than 1% of all CVEs reside on endpoints and are also under attack–in all, only about 1,500 CVEs have been observed on endpoints and in IPS activity simultaneously. This is excellent news for CISOs as it gives them a clear view of the active attack surface, simplifying management.

Red Zone

This data allows us to introduce a new baseline for measurement. Let's call it "the red zone," or the percentage of current CVEs under active attack during the second half of 2022. As you can see above, most CVEs were not observed on endpoints (dark purple), and among those observed (yellow), even fewer were also under attack (red). To calculate the red zone, you take the number of active attack surfaces (where CVEs are observed and under attack) and divide them by the total number of CVEs on endpoints. The case above shows that the **overall red zone for H2 2022 is 8.9%**.

For more insight, let's explore a single vendor-level comparison between Apple and Microsoft:

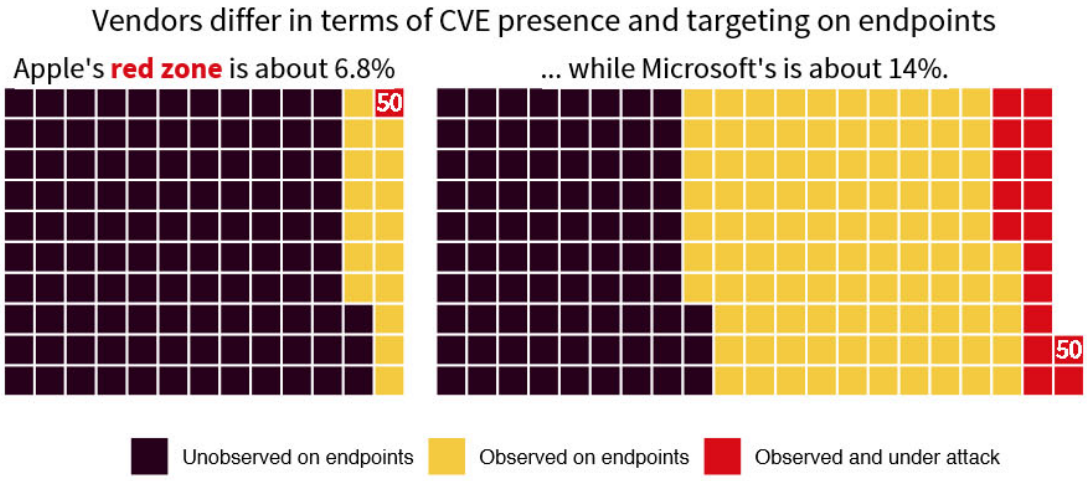

Figure 9 - Comparing all Apple and Microsoft CVEs by their presence on endpoints and in IPS telemetry

Right off the bat, we can see some stark differences here, even before we start talking about the red zone. Most of Apple's CVEs were not observed on endpoints, making the proportion of observed and observed and under attack much smaller than Microsoft's. Conversely, over half of all Microsoft CVEs were observed on endpoints in the second half of 2022. So, the two vendors not only have different active attack areas, but we also have a better idea of how much is potentially at risk for each solution.

Based on how we calculated the red zone for our overall plot in Figure 9, we can see that Apple's red zone is about 6.8% (below average), while Microsoft's is about 14% (above the norm).

While it's comforting to see that not all of Microsoft's vulnerabilities are being targeted, protecting against the attacks that leverage them is not as simple as placing a few definitions in static defenses. While static definitions are produced daily for perimeter security solutions like next-generation firewalls (NGFWs), it's dynamic defenses like sandboxing and EDR that are most effective at stopping attacks based on their real-time AI/ML machine learning capabilities coupled with deep neural network intelligence and virtual patching capabilities that continuously reduce the attack surface.

Of course, the big question remains–how can defenders determine which open CVEs might enter an attacker's crosshairs? You might assume that more CVEs seen on targets mean more attacks, but we have found very little correlation between IPS activity and presence on endpoints, even when accounting for severity. Figure 10 below shows the volume of IPS activity and presence on endpoints for any CVE that appeared in both datasets.

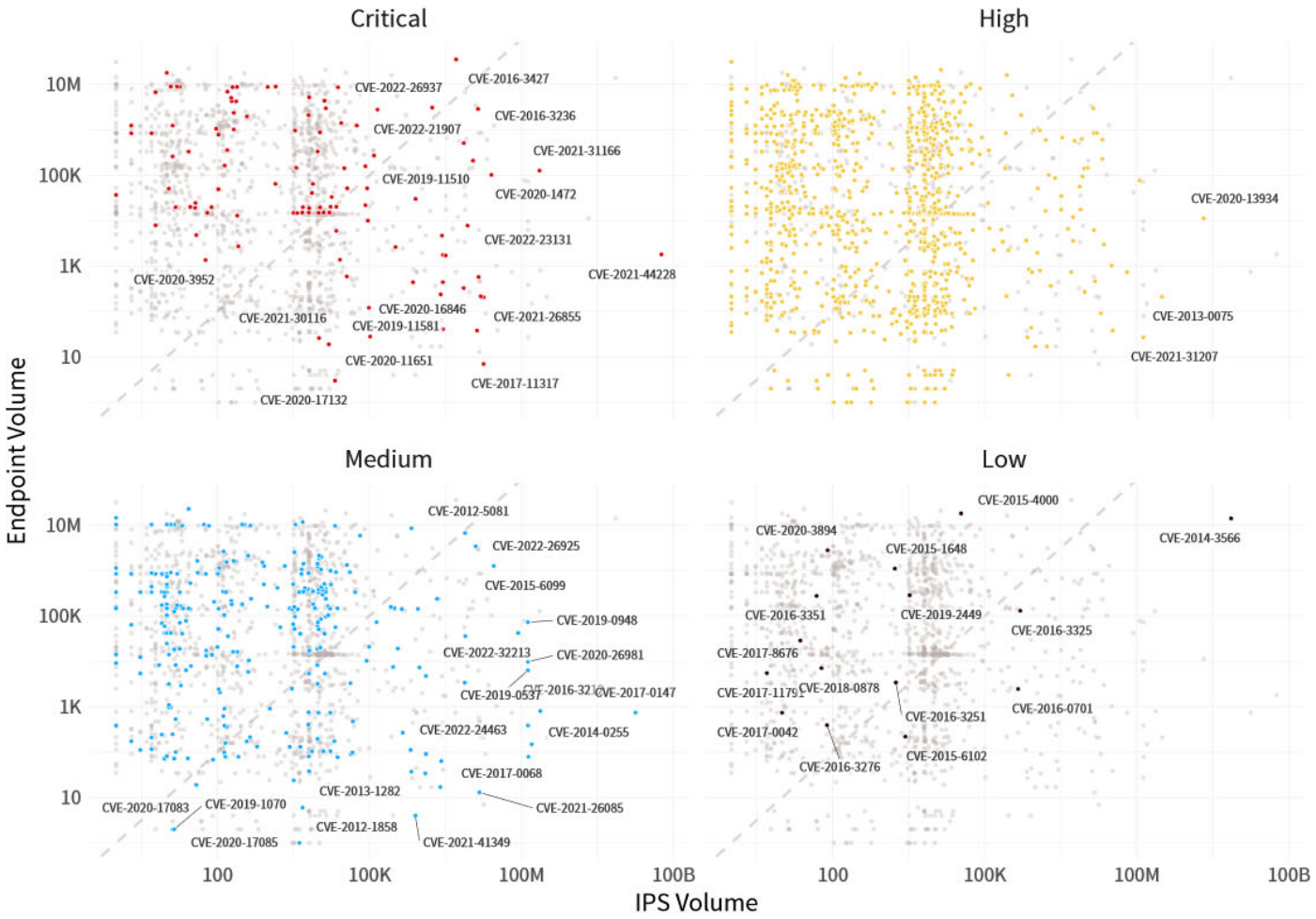

Figure10 - CVEs by their presence on endpoints and in IPS telemetry for 2H-2022, organized by severity

If attackers prioritize CVEs based on their presence on endpoints, we'd expect most points in the graph to lie along or below the diagonal line. Instead, we see many CVEs that are abundant on endpoints but sparse among attacks. That's because attackers consider many factors when selecting their targets, but an abundance of exploitable CVEs doesn't appear to be one of them. Let's look at a graphic that shows the prevalence of attacks against platforms, taking into consideration every organization that detected an exploit attempt.

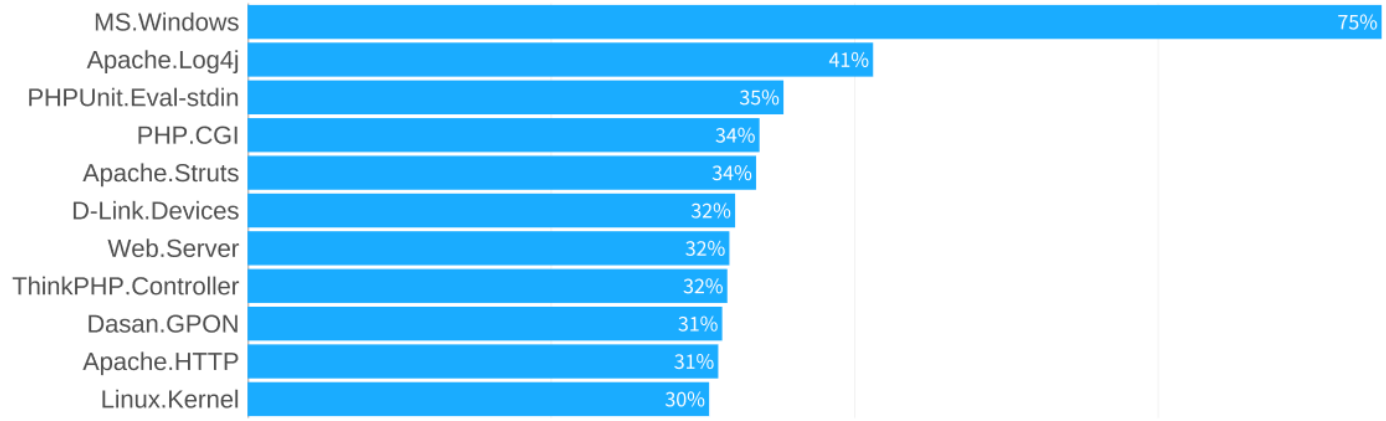

Figure 11 - Prevalence of top IPS detections by platform

During the second half of 2022, MS.Windows rose to the top of IPS threats, with 3 out of 4 organizations detecting related activity. However, not to be forgotten, Log4j (the Apache server vulnerability that achieved worldwide notoriety at the end of 2021) is still widespread with the PHPUnit.Eval-stdin vulnerability from 2020 following closely behind. But let's go back to MS.Windows for a moment, as it was by far the most prevalent IPS threat of the second half of 2022.

Microsoft jumped from 32.9% to 84.4% between July and August, knocking Apache from its number-one spot. While many others also experience rises and falls, this one caught our attention. Let's look deeper into all organizations that detected Microsoft exploitation attempts to see which vulnerabilities were more targeted.

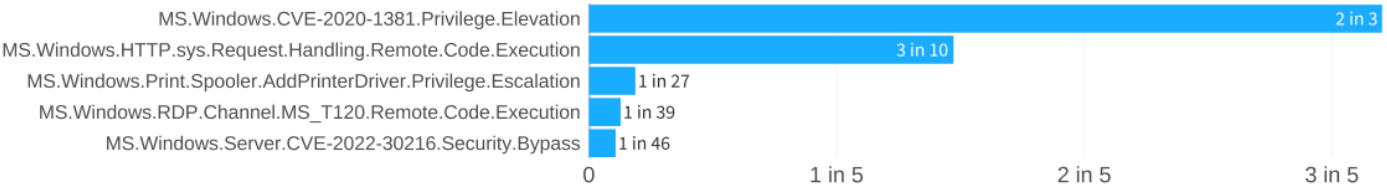

Figure 12 - Top 5 Microsoft-specific IPS detections

When we examine the MS.Windows threats, we see that MS.Windows.CVE-2020-1381.Privilege.Elevation is a privilege escalation vulnerability that exists in Win32K. This vulnerability is due to an error in a vulnerable application when it handles a malicious file, allowing a remote attacker to exploit and then leverage their privileges on this system. It's a vulnerability that has been disclosed for over two years. Yet, it still seems to be the preferred method for malicious users since they can exploit so many vulnerable (i.e., unpatched) devices.

Then we have MS.Windows.HTTP.sys.Request.Handling.Remote.Code.Execution, first discovered back in 2014. This vulnerability is due to an improper boundary check in the protocol. It can allow a remote attacker to utilize this exploit to execute code within the application through an HTTP request.

And MS.Windows.Print.Spooler.AddPrinterDriver.Privilege.Escalation, an exploit in the Microsoft Windows Print Spooler, is one of the newest vulnerabilities we saw during the second half of 2022.

The Long Reach of Log4j

There's still the issue of Apache. Let's see where Log4j was most prevalent during the second half of 2022.

	Africa	Asia	Europe	N. America	Oceania	S. America
Technology	13.4%	10.4%	11.0%	9.9%	12.1%	12.0%
Government	8.1%	3.2%	5.1%	5.4%	5.2%	7.9%
Education	3.2%	3.6%	3.7%	8.0%	8.6%	4.5%
Banking/Finance/Insurance	13.2%	5.1%	3.5%	4.5%	3.9%	4.8%
Manufacturing	3.9%	7.3%	6.6%	5.7%	3.4%	4.5%
Healthcare	2.9%	2.9%	4.6%	6.8%	5.2%	4.4%
Retail/Hospitality	2.1%	2.5%	2.0%	2.2%	2.7%	2.1%
Energy & Utilities	2.6%	1.4%	1.9%	1.5%	1.3%	2.4%
Construction	1.3%	1.3%	2.3%	2.6%	2.9%	2.2%
Transportation and Logistics	1.7%	1.9%	2.1%	1.4%	1.8%	3.0%
Consulting	1.7%	1.1%	1.9%	2.1%	1.8%	1.8%
Telco/Carrier	3.0%	1.2%	1.1%	0.7%	2.0%	2.0%
Food & Beverage	1.1%	1.3%	1.5%	0.9%	1.0%	2.0%
Nonprofit	1.0%	0.7%	1.0%	2.7%	3.0%	0.5%
Media/Communications	0.8%	0.9%	1.6%	1.2%	1.6%	1.1%
Agriculture	1.3%	0.5%	0.6%	0.5%	1.0%	1.9%
MSSP	0.9%	0.3%	0.7%	1.2%	1.8%	0.4%
Automotive	0.8%	0.8%	1.3%	0.7%	0.9%	0.9%
Legal	0.7%	0.2%	0.5%	1.4%	1.0%	0.6%
Environmental	0.3%	0.3%	0.4%	0.3%	0.7%	0.4%

Figure 13 - Percent of organizations seeing Log4j attacks by region and industry

Log4j-based attacks heavily favored the technology industry, regardless of region, primarily because Apache Log4j is such a popular open-source software. Because it can be so deeply embedded into various applications, many companies might not even be aware that they have built their current systems on top of a Log4j component. It is deployed even in places you never thought of, such as Ghidra (a debugger), where it has been fully incorporated. Because of its widespread use, we assume it will continue to be used for a long time. After the Technology sector, Africa's Banking and Finance industry is the next most targeted.

Rookie of The Half

In each report, we award the title of "Rookie of the Half" to a vulnerability discovered in the past 12 months that also showed the highest prevalence among organizations during the recent half.

VMWare's Workspace One Access Catalog vulnerability, which surfaced in July 2022, is a critical remote code execution vulnerability that was first noticed in mid-2022 when the vulnerability first became apparent during a server-side injection flaw. The nodes that were seen through this vulnerability seem to be similar to those of generic botnets. Another interesting thing to note is that three of the top six Rookies of the Half are Spring related. If "Spring" sounds familiar, it's because the Spring framework had two zero-day vulnerabilities reported during 2022. While they aren't highly prevalent, keeping these vulnerabilities in mind as we move forward this year is a good idea.

Protecting against (0-day) vulnerabilities starts with the question, "what do we need to protect?" But the response will always be a combination of network-based and endpoint-based detection and protection methods. Both should include the latest security updates and threat intelligence provided by a global threat research team to ensure complete visibility across all regions and industries.

- Next-Generation Firewall with IPS to protect IT/OT/IoT devices on the network
- Web Application Firewall with IPS to protect Web Servers
- DataCenter Firewall with IPS to protect servers and workloads
- EndPoint with IPS to prevent the OS and applications from being exploited
- Sandbox technology to detect advanced and new TTPs and exploits.
- Deception technology for early detection of customer-targeted and specific TTPs and exploits.

Malware

Most Active Malware Groups

Malware has a way of dominating headlines and keeping businesses on their toes. From Ransomware to InfoStealers to Wipers, late 2022 was a period of uncertainty, especially as we saw wipers deployed to Ukrainian organizations during the Russian invasion of Ukraine. This is likely a first where an adversary invaded a country and deployed destructive malware simultaneously. In fact, when writing this report, news outlets were reporting that Ukraine has called for the equivalent of a Cyber United Nations to aid in sharing threat intelligence amid continuous Russian cyberattacks.

2022 also marks the 10th anniversary of Ransomware in its modern form, an anniversary many aren't likely to celebrate. We decided to provide a recap. Reveton debuted between 2011 and 2012. It was the first modern ransomware to present an intimidating lock screen and payment options such as Moneypak, MoneyGram, and Green Dot to unlock files. And following closely behind is the tenth anniversary of Cryptolocker, the first ransomware to request payment in Bitcoin.

Some of those threat actors also landed in the notorious Advanced Persistent Threat (APT) category. Lazarus (15%), OceanLotus (10%), and Sofacy (7.9%) are the top three in our APT chart: our hash telemetry, enriched with malicious code mapping, allows us to dig deeper into the most active codebase found in the wild on these hashes. Of course, APT groups frequently use a large number of malicious payloads. But because the delivery code is being reused, we decided to simplify and provide details at a higher level. In the following image, we showcase the amount of code found on all samples we observed, breaking them down by APT.

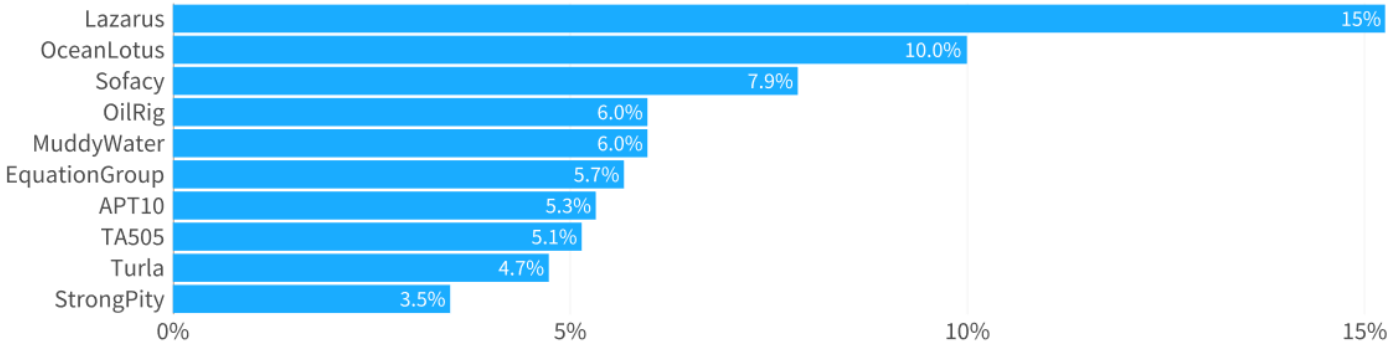

Figure 14 - Top APTs observed

Lazarus, also known as HIDDEN COBRA/APT38/BeagleBoyz, is a cyber group attributed to the government of North Korea. It has been linked to multiple high-profile, financially motivated attacks in various parts of the world–some of which have caused massive infrastructure disruptions. Some past attacks worth noting include the 2014 attack on the U.S.-based division of Sony Entertainment, where emails, employee data, unreleased movies, and confidential data were stolen. This was allegedly in retaliation to the proposed release of the comedy, The Interview, which mocked the leader of North Korea. In addition to leaked data, acts of terrorism were threatened against Sony and its partners, ultimately delaying the film's release. Another significant attack involved a 2016 Bangladeshi financial institution heist that almost netted nearly $1 Billion (USD) for the attackers. Fortunately, a misspelling in the instructions caused a bank to flag and block thirty transactions. Otherwise, Lazarus would have pulled off the biggest heist of its kind. Although they failed in their larger attempt, they still netted around $81 Million.

Another high-profile attack attributed to Lazarus was the infamous Wannacry Ransomware attack, which resulted in massive disruption and damage worldwide to thousands of organizations, especially those in manufacturing. The impact also resulted in the loss of hundreds of millions of dollars, some claiming the loss of billions. Other verticals targeted included critical infrastructures, entertainment, finance, healthcare, and telecommunication sectors across multiple countries. Lazarus has been the subject of numerous governmental agency advisories due to their variety of attacks. Their latest, Operation In(ter)ception, used a fake Coinbase job posting to lure targets to unknowingly install a MacOS malware that enabled them to conduct espionage and ultimately steal cryptocurrency.

Following closely behind Lazarus is OceanLotus. Active since 2014, **OceanLotus** is a state-sponsored group out of Vietnam that targets organizations of interest to the Vietnamese government. In late 2022, reports connected OceanLotus to a string of zero-day attacks using the Torii IoT botnet in China.

Then there's **SoFacy**, otherwise known as Fancy Bear, Sednit, and PawnStorm (a group from Russia), which has been around since at least 2008. It has typically targeted political groups, governments, and defense industries. In late 2022, SoFacy was observed sending malicious documents that contained the exploit for Microsoft's Follina zero-day vulnerability.

So, does the trend of older threats maintaining and expanding their foothold carry over to malware families? Based on our telemetry, we could see almost 500 (482, to be exact) active malware families in the wild. Let's take a look at the most active:

Did You Know

In 2022, a total of over 20 million successful brute force attacks were recorded by our system. Read our blog to learn more about IoT Threats

SoFacy/ Follina 0-Day?

We've got you covered.

Right after announcing a new zero-day at the end of May, FortiGuard Labs released protections across the Fortinet Security Fabric to stop the attack on the MITRE delivery, exploitation, and Installation phases with AV, IPS, and Post-execution signatures.

Learn more about the Follina Outbreak Alert here

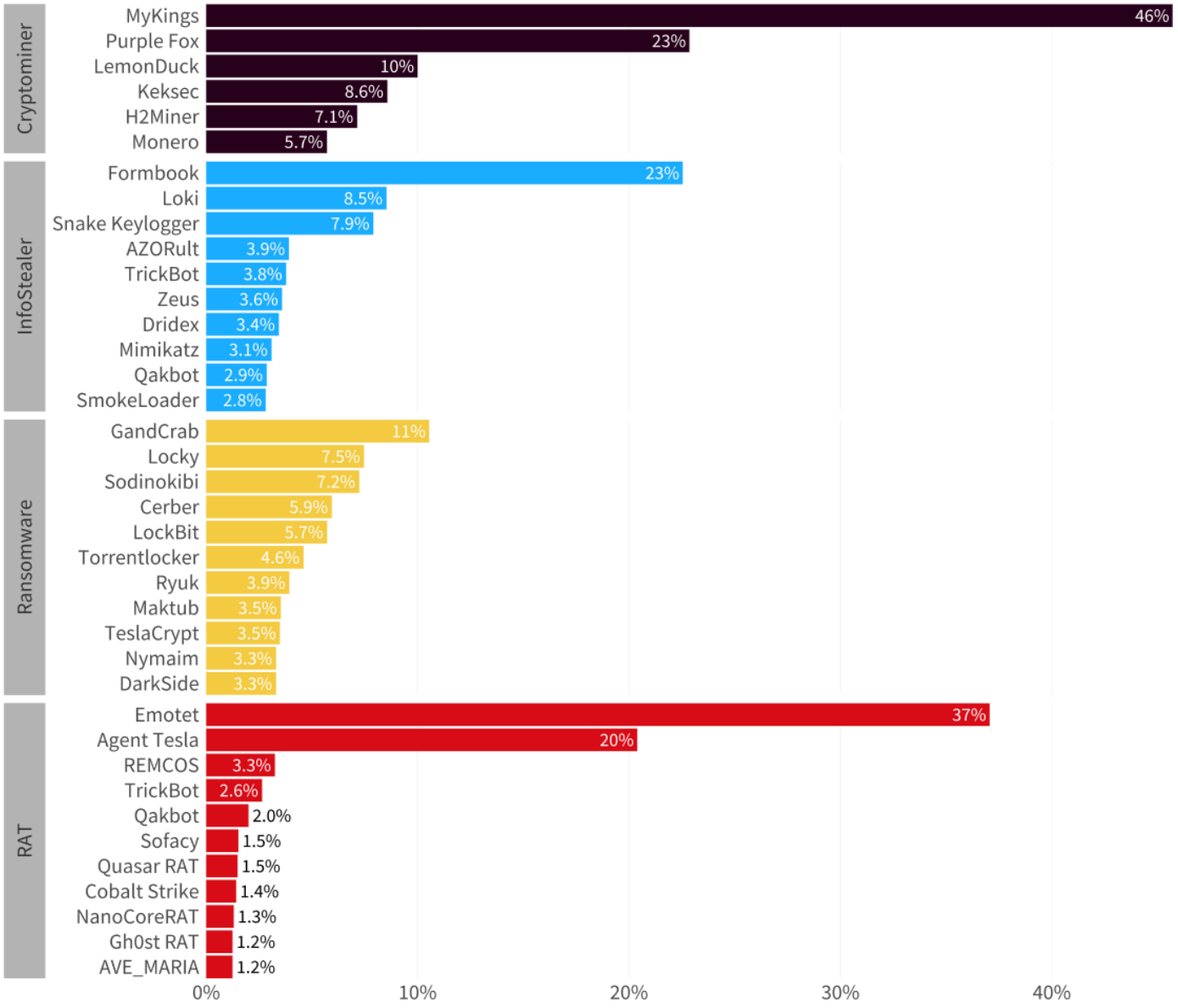

Figure 15 - Top families by malware type

At first glance, we start to see some interesting things:

- First, the top five ransomware families (out of 99) account for about 37% of all ransomware activity in late 2022.
- GandCrab, a Ransomware-as-a-Service, first emerged in 2018. Then in mid-2019, after making over $2 billion in profits, the criminals behind it announced they were retiring. However, it is believed that these actors disbanded only to regroup as REvil and Sodinokibi. REvil was credited with the Colonial Pipeline and JBS Foods attacks (to name a few). And while authorities temporarily took down REvil in Russia, including some arrests in 2022, the group appears to have regrouped again and is continuing operations.
- For cryptomining, MyKings claimed the top spot for late 2022. MyKings, or Smominru or DarkCloud, has primarily targeted Windows-based users since 2016. They continue to be a formidable cryptominer by building redundancy into their malware process and quickly adding new capabilities, such as when they used a photo of Taylor Swift to launch a new update to their cryptominer.

We also see a familiar name at the top of the RAT (Remote Access Trojan) category–Emotet. Although not technically a RAT, Emotet has incorporated so many capabilities and modules that parts fall squarely into the RAT category. Discovered in 2014, its creation has been attributed to the cybercrime group TA 542 (also known as Gold Crestwood and Mummy Spider). It first emerged as a banking Trojan that attempted to gain access to a computer and steal personal information. Over time, however, the banking Trojan evolved into its current iteration as a malware distribution botnet. Emotet is spread via spam messages, and once it gains access to a system, it continues to spread by connecting to the system's contacts list. Emotet went offline briefly in January 2021, only to return with a vengeance in November 2021. It is believed that Conti, the notorious group based out of Russia, utilized the Emotet botnet until they were shut down in May 2022.

Emotet is resilient because it relies heavily on polymorphism for its packer, enabling it to easily bypass legacy AV technologies. The group behind Emotet is also evolving its behavior, tweaking strategies to evade detection and improve the chance that its target audience will open its spam emails. Once it takes over a machine, it uses the victim's email address and inbox for future attacks.

Determining the exact percentage of organizations utilizing advanced cybersecurity technologies is difficult. This can vary due to several factors, such as the organization's size, industry, and location. However, one recent survey estimated that less than 40% of enterprises had adopted some form of advanced cybersecurity detection and response technology, such as EDR and SIEM enhanced with machine learning (ML), to address advanced threats. This percentage is likely even lower for smaller organizations. For example, most of our Incident Response engagements show that the client did not have an EDR technology in place. They just had legacy AV and no real visibility into the threat activity in their environments. While these numbers are far too low, trends indicate that advanced technologies are slowly being adopted in response to the evolution and growing sophistication of cyber threats.

It's important to note that while implementing such technologies increases detection, prevention, and automated response coverage, they do not guarantee success. Organizations still need a comprehensive cybersecurity strategy that considers their specific needs and risks. People and processes must always come before technology, so make sure you understand what is required for your environment and apply best practices across your entire attack surface (such as providing security awareness and cyber training for employees) before you go cybersecurity shopping.

The majority of our Incident Response engagements support this view. Very few impacted organizations clearly understood the issues they needed to address, active programs to uplevel employees' skills, or even full implementation of the products they needed to defend themselves (best practices), such as having EDR and NDR technology in place.

Fortunately, there are many services and tools available for organizations to improve and evaluate their cybersecurity posture and readiness across all three disciplines:

OLD SIGs Never Die

FUN FACT: All the hashes associated with this cryptominer were blocked by our 2016! AV signatures across the Fortinet Security Fabric

FortiGuard Antivirus delivers automated updates that protect against the latest threats

SPAM ALERT:

Watch out! It's growing faster than a weed at 100% per year!

Phishing attempts, sophisticated techniques that avoid detection, combined with the sheer volume of SPAM received daily help organizations realize that e-mail security is still a cornerstone in their cyber strategy.

FortiMail helps your organization prevent, detect, and respond to email-based threats like spam, phishing, and malware including ransomware, zero-day threats, impersonation, and business email compromise (BEC) attacks.

- Early Detection
  - Deception and Reconnaissance
- Protection
  - AI-Powered AV and IPS
  - AI-Powered Inline Sandboxing service from the cloud
- Detection and Response
  - End Point Detection and Response (EDR)
  - Network Detection and Response (NDR)
- Re-design and Architectural Changes
  - Network and micro-segmentation to allow for identification of lateral movement.
  - Zero Trust Access
- Validation, Training, and Awareness
  - Incident Readiness and Response services
  - Security Awareness training

Malware Code Reuse

When we looked at the top malware for the second half of 2022, most were over a year old. Some were even considered "ancient" by cybersecurity standards.

Many legitimate software projects reuse code to build new applications on a solid foundation while making room for changes. Further, each iteration has the opportunity to spin out and become something in its own right–and its code can likewise be built upon, changed, and re-released.

So, what does it look like when malicious users do this to their malware? Let's investigate one example: Emotet.

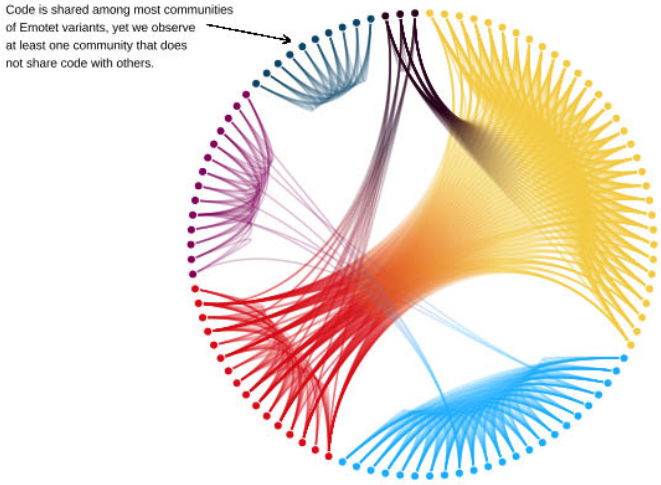

Figure 16 - Code reuse within and across communities of Emotet variants

THE AI/ML Effect:

Blocking new or morphed malware in near real time

DID YOU KNOW? Our AV engine combines an automated content pattern recognition language (CPRL) with machines teaching other machines to dynamically build AV Signatures and find new malware variants based on shared code, something we refer to as a 'Real Time Sandbox.' Our Advanced Threat Protection (ATP) Framework is unique in the industry, leveraging integrated solutions to make autonomous decisions based on threat intelligence. In-line Sandbox technology is available on the network, cloud, endpoint and email security layers.

See what our CTO and Co-founder Michael Xie had to say about it here

We examined a collection of 98 different Emotet variants and analyzed their tendency to "borrow" code from one another. We found that in the nearly a decade since it first reared its head, Emotet has undergone a lot of speciation. Using some fancy network community detection algorithms, we found that these 98 variants can be broken into roughly six different "species" of malware, shown in the Figure above.

Each point in the figure is a different malware variant. Colors indicate an inferred community, and the arcs between points show the amount of code reuse. The yellow community is highly connected, sharing a significant portion of its code with itself and other variants. The other five smaller communities (except for the dark blue community in the top left) share some code among groups but mostly have unique code bases and only share bits and pieces with other variant communities. Then there are the two communities that only share code between themselves (purple and light blue). An in-depth analysis of what the shared code does is out of the scope of this document, which aims to only provide higher-level insights into the threat landscape.

Mitigating Code reuse and the frequency of variants is a battle of time. How fast you can protect, detect, and mitigate such threats defines the effectiveness of your security posture and your capabilities to keep your adversaries out.

Deploying modern AV, tightly integrated with AI-powered In-Line Sandbox technologies, is a necessity. The power of a cybersecurity fabric lies in the native integration of its layers of protection and the ability to enforce policy consistently across your organization. Critical protections like email, endpoints, networks, and clouds must be automated and centrally orchestrated. That way, when architectural designs change, implementing things like segmentation across the distributed network makes it easier to identify and prevent lateral movement across your infrastructure.

Lastly, Machine Learning-enabled analytics will help correlate 'anomalous' behaviors into an alert that needs triage. Operationalizing the MITRE ATT&CK system on your adversaries' TTP profiles and continuously testing novel techniques against your cybersecurity solutions is necessary for organizations committed to defending their environment. Attack simulation tools and services can help identify gaps and close them.

Ransomware

To compare ransomware activity over time, we dug into our virus data. Comparing monthly volumes shows noticeable growth from the first to the second half of 2022–about 16%–despite some drastic month-to-month variation. Most of this seems to be due to an influx during July and August.

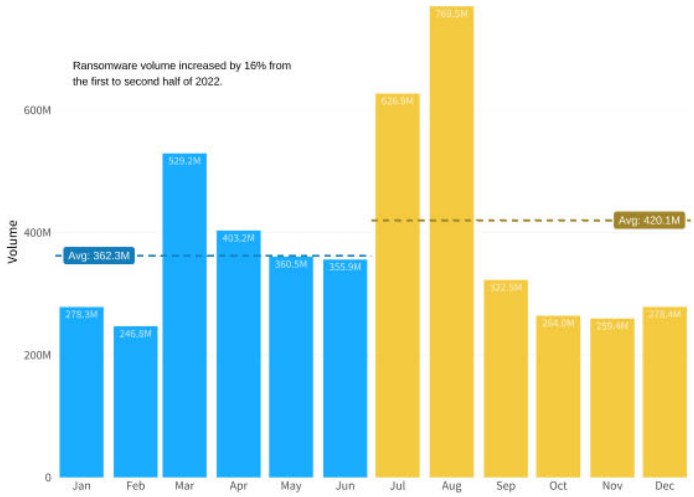

Figure 17 – Monthly ransomware volume for 2022

The gradual increase in average volume, combined with a quick readjustment after August, resembles a pattern we've seen before. It's the traditional whack-a-mole game in ransomware being played out in 2022, where some ransomware deliberately halts activities, and brand-new ones arise to replace them. Here are two ransomware groups that caught our attention during the year.

Royal Ransomware was new in 2022 and picked up notoriety as the year went on. In its ransom note, the ransomware threat actor not only asks victims to pay a ransom for file decryption and prevent stolen files from being leaked to the public but also offers penetration testing and security review services for a fee. Recently, the developer added a new variant targeting Linux platforms, indicating the time and effort spent on ransomware development.

In November, we also reported on the new **Cryptonite** ransomware. It came as a builder and server combination for easy use and deployment. The builder allows cybercriminals to generate a Cryptonite ransomware built with a custom configuration, such as an attacker's Bitcoin wallet address, the amount of Bitcoin to ransom, a contact email, and a file extension for the encrypted files (the ".cryptn8" file extension is set by default). As Cryptonite is an open-source ransomware, anyone can use it. Note that the hosting webpage is no longer accessible after we publicly reported the ransomware.

The good news is that the multi-vector, multi-stage nature of ransomware campaigns provides multiple opportunities for organizations to thwart attacks before their endgame. Strong protections across the digital attack surface that leverage AI-powered security services from the cloud to block known attacks, combined with in-line protection of unknown components using Inline Sandbox and Network Detection and Response, help reduce the likelihood of entry. But even if intruders do make it in, strong behavior-based detection, such as EDR on a device, Detection & Response and Deception technologies on the network, and Digital Risk Protection (DRP) for insight into the dark web can trigger a fast response–especially when combined with centralized monitoring and an orchestrated response provided by SIEM or SOAR technologies as appropriate. In addition, many cybersecurity companies now offer augmentation services for organizations needing more SOC-specialized staff to effectively evaluate and protect the organization. Fortinet has experts trained to augment the abilities of your in-house teams.

Does Your Short-Staffed Security Operations Team Need help?
Fortinet SOC Augmentation Services Provide Immediate Support via:

- SOC as a Service (SOCaaS) blends FortiGuard cybersecurity experts with Fortinet advanced SOC technology that includes artificial intelligence (AI) and machine learning (ML) capabilities to support most use cases. This enables Fortinet to speed up alert triage, rapidly escalate security incidents, and reduce false-positive alerts.
- Outbreak Detection Service alerts subscribers through email–and automatically within key product user interfaces–to major breaking cybersecurity events that have the potential for widespread ramifications. These alerts include critical information about security incidents, such as an attack's timeline of events and what specific technology has been affected. In addition, the alerts provide organizations with custom threat hunting to run against logs and identify the potential impact of an attack, along with recommendations to improve your security posture for better protection in the future.
- Incident Response and Readiness (IR&R) Services. Our proactive prevention-oriented services, such as risk assessments, playbook development, and tabletop exercises–all part of an Incident Response and Readiness Services retainer–help organizations strengthen their cyber preparedness and SOC effectiveness while reducing cyber risk. It also provides access to a team of FortiGuard experts that can help with rapid containment and remediation in the event of a cyberattack. In response to an accelerated demand for such services around the globe, Fortinet is expanding its headcount dedicated to IR&R and SOC automation capabilities to allow more enterprises to access the offering.
- Fortinet's Managed Detection and Response (MDR) service provides advanced threat detection, proactive threat hunting, rapid incident response, comprehensive reporting and analysis, and continuous improvement to help companies better detect and respond to breaches in their environment. The MDR service uses AI and ML algorithms to identify potential threats and is continuously updated to stay ahead of the latest threats. The service includes a 24/7 SOC staffed with security experts who can quickly and effectively contain and remediate any security incidents. Detailed reports on security incidents can be used to improve security processes and provide evidence of compliance with industry regulations and standards. The MDR service is continually evolving to stay ahead of the latest threats.

Wipers

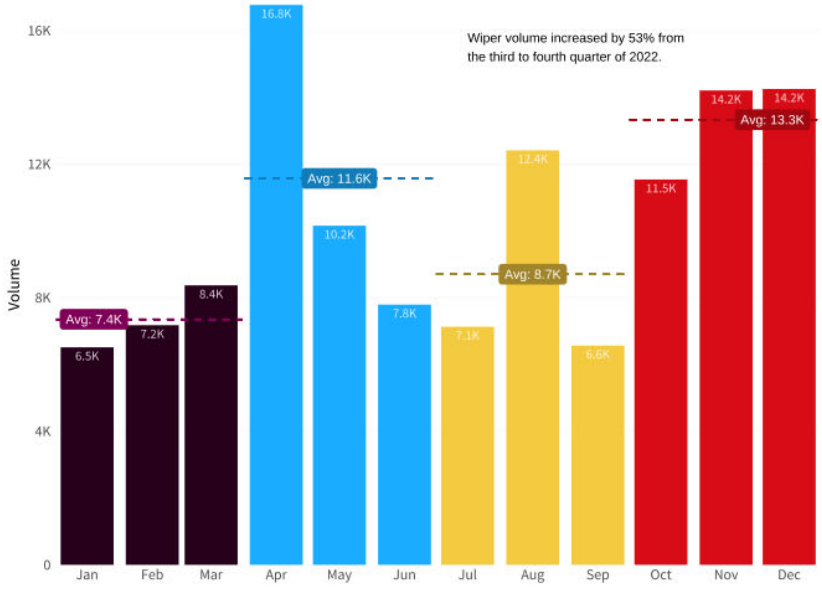

Figure 18 - Quarterly wiper volume for 2022

Wipers also saw an increase in volume between the first and second halves of 2022, but they ended the year with a distinctly upward trajectory. Wipers–so named because the malware tends to "wipe" the victim's computer data–have been around since 2012. However, an interesting difference in the first half of 2022 was that most of the discovered wipers (WhisperGate, HermeticWiper, CaddyWiper, etc.) were publicly attributed by many organizations to Russian state-sponsored actors. And in the second half, newly discovered wipers were either attributed to pro-Russian hacktivist groups such as Somnia or individuals inspired by the wiper trend began creating their own wiper malware.

Worryingly, we see a 53% increase in wiper volume when we compare the third to the fourth quarter. After an initial spike in August, we see another jump in November while December maintains the same volume. Even though the peaks for the second half are noticeably lower than the one prominent peak in the first half of the year, wiper volume has clearly risen over the year, and it doesn't look like it will be slowing down any time soon.

In early 2022, we also reported the presence of a few new wipers that popped up in parallel with the Russia-Ukraine war, but those new wipers seem to operate without borders.

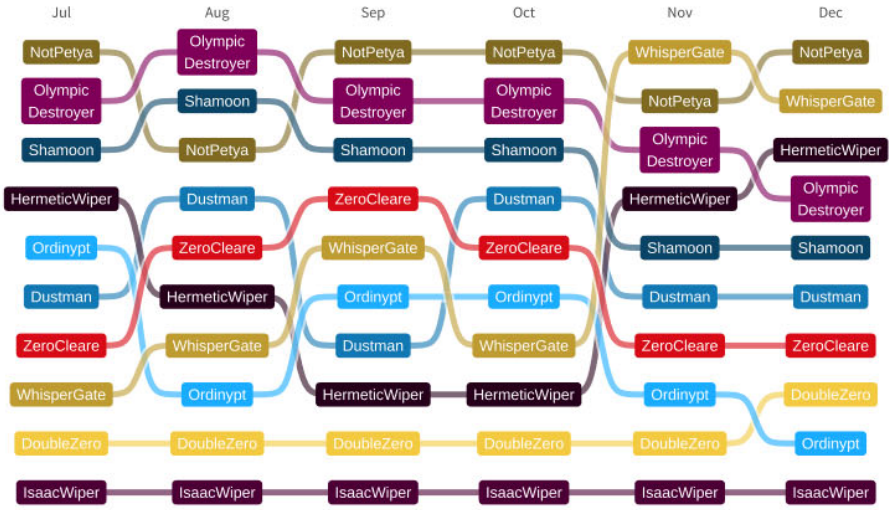

Figure 19 - Monthly ranking of wipers by prevalence (top being the most prevalent)

There's not much shuffling among the top wipers in terms of prevalence–i.e., the proportion of organizations seeing them. Almost all the wipers experienced an increase in November 2022, consistent with the previous Figure. In January 2022, it was reported that there was another attack against Ukraine, known as WhisperGate, which slowly spread until it became the top wiper in November 2022. It's believed that Russian Military Intelligence is behind the development of this wiper.

One wiper to keep an eye on is HermeticWiper, initially discovered in late 2021 when it was believed to have been used by Russia against Ukrainian targets. We saw a significant spike in HermaticWiper in November, which became even more prevalent in December. This wiper targets the victim's Master Boot Record (MBR) and has reportedly affected organizations in Ukraine. Much like our previous report, the top wipers appear opportunistic. WhisperGate and HematicWiper have their highest prevalence outside of Europe, even though that's not where their most prolific attacks have been. North America, overall, seems to see the least wiper activity. The lack of borders on the Internet allows criminals to do whatever they want without constraints.

	Africa	Asia	Europe	N. America	S. America
WhisperGate	75%	62%	74%	44%	71%
NotPetya		92%	74%	56%	71%
HermeticWiper	25%	85%	73%	44%	57%
Shamoon	25%	69%	62%	56%	43%
DoubleZero	50%	46%	64%	22%	71%
IsaacWiper	25%	54%	54%	11%	57%
Dustman		62%	60%	22%	43%
ZeroCleare		62%	60%	22%	43%
Olympic Destroyer		54%	68%	22%	43%
Ordinypt		46%	59%	11%	43%
CaddyWiper	25%	15%	14%	22%	
WhisperKill		15%	12%	22%	
Azov			15%	11%	14%
AcidRain		15%		22%	

Figure 20 - Percent of organizations seeing each wiper by region

So, does the data support the idea that the increase in wipers is because of the ongoing war in Europe? Yes. And with the majority of wiper activity coming out of Russia, one could expect more wiper use being targeted at nations and companies supporting Ukraine with weapons, aid, or other logistics. We are seeing a new breed of wipers in 2H, with some now open source and on GitHub. Since some wipers emulate ransomware activity, they are usually detected and defused in real time before they can fulfill their add-on objectives by endpoint detection and response (EDR) technologies. As a result of this increase in ransomware, espionage, malware, and wipers, many national and local government agencies have prioritized their acquisition of EDR technology.

Cybersecurity professionals are constantly searching for the "next big thing" to help in the battle against wipers and ransomware.

Off-side and Off-line Backups: The most helpful countermeasure for ransomware and wiper malware is to have backups available. However, malware often actively searches for device backups on the machine (such as Windows Shadow Copy) or the network to destroy, so backups must be kept off-network.

Segmentation: Proper network segmentation can be helpful on multiple levels. For example, it can limit the impact of an attack to one segment of the network. In addition, firewalls combined with anti-virus and intrusion prevention systems can detect the propagation of malware on the network, communications to known command and control servers, and malicious files as they move through the network.

Incident Response: The speed and quality of incident response are crucial, and the outcome of an attack can highly depend on them. When a compromise is detected before wiper malware is deployed, how the incident response team handles and responds to this alert could mean the difference between successfully averting data loss and complete data destruction.

Execution, Persistence, and Defense Evasion

Targeting endpoint security software highlights its threat to cybercriminal operations while providing organizations with another opportunity for early detection. An essential technique offering a significant return on investment is looking for the degradation of security tool coverage when monitoring environments. In ~56% of incidents, the FortiGuard IR team identified threat actors disabling local security software. As shown in Figure 21 below, this was the most commonly observed Defense Evasion technique used for intrusions investigated by the FortiGuard IR team in 2022.

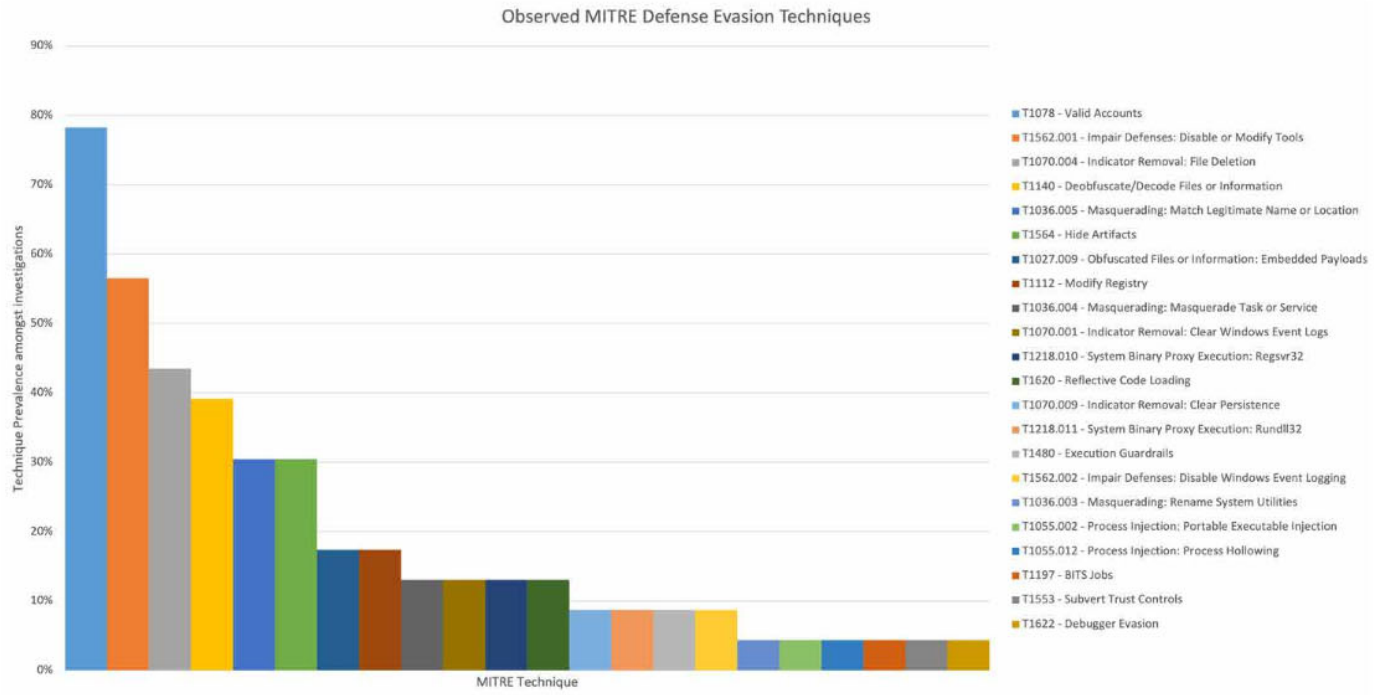

Figure 21 - MITRE Defense Evasion techniques observed by the FortiGuard IR

In most cases, this technique was employed early in an intrusion. This makes it a great candidate for defending networks, as detections earlier in the kill chain give IT teams more time to apply mitigations before adversaries can complete their actions on objectives. This technique is often implemented by looking for AV services such as Microsoft Defender and FortiClient and stopping them through simple PowerShell commands. Another common method uses the third-party tool 'Defender Control,' which was explicitly designed to disable Windows Defender. The FortiGuard IR team has seen consistent usage of this tool between affiliates associated with multiple ransomware groups, so while it may be flagged as a Potentially Unwanted Program (PUP), anomalous detections of the tool should be investigated thoroughly.

Many modern endpoint security products operate as services monitoring the status of security product services running in your environment and then investigating any outages promptly. This can also lead to the early detection of intrusions. Service modifications can be monitored by centralizing default Windows security logs and checking for records using event id 7040, which references a change of state for installed security. Similarly, most advanced EDR solutions are resilient against such simple security product bypasses. They also detect attempts to disable Windows Defender through the methods described above.

Another common technique employed across intrusions and threat actors is creating a malicious service. The use of malicious services is growing in prevalence by offering Execution, Persistence, and Privilege Escalation opportunities through a single solution. As can be seen in Figure 21 above and Figure 22 below, the use of Windows services for execution and persistence was observed in >30% of cases.

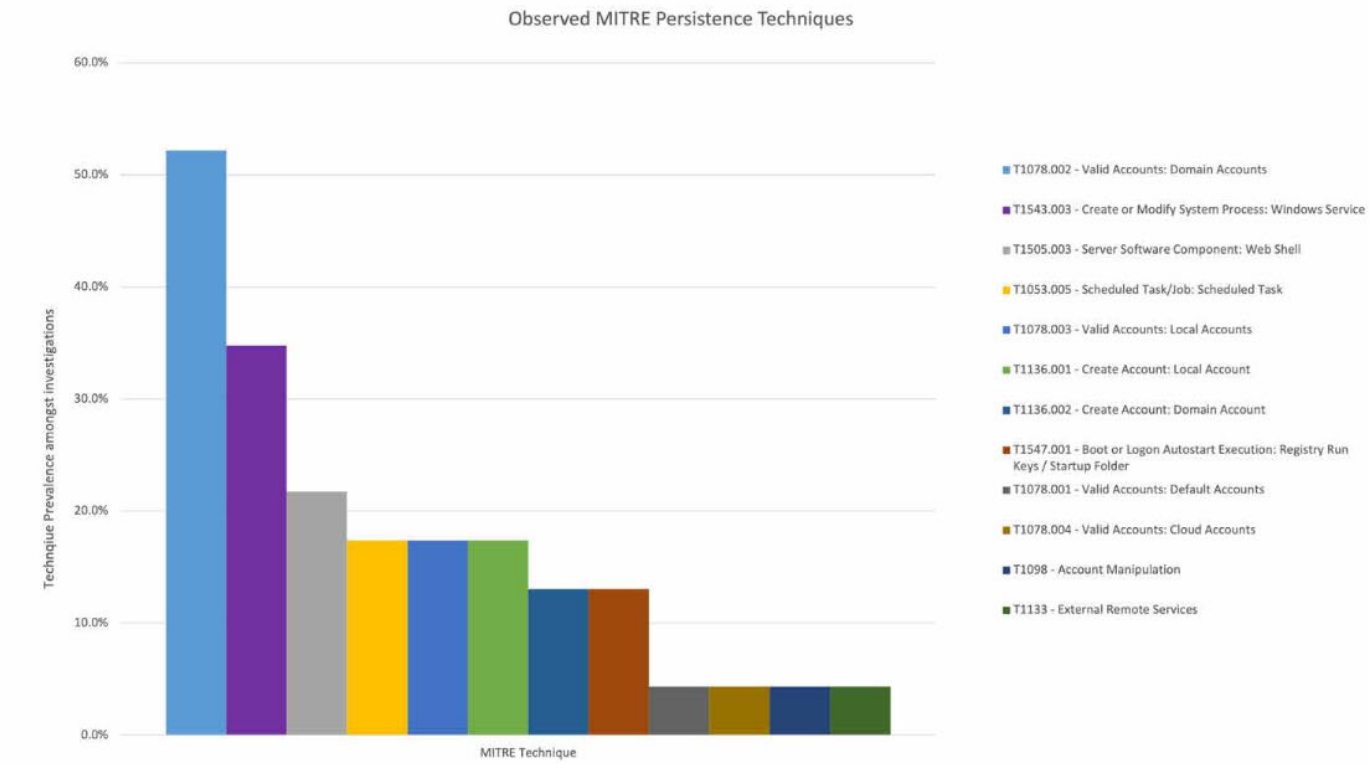

Figure 22 - MITRE persistence techniques observed by the FortiGuard IR team throughout 2022

The use of malicious services is likely so widespread for several reasons:

1. It disassociates the execution of malware or malicious scripts from an adversary's implant process chain. For example, if an adversary has established a Cobalt Strike beacon within an 'explorer.exe' process (via process injection), executing additional malware from the Explorer process may draw attention due to anomalous process chains spawning from Explorer. By executing malware through a service, it is executed from the services process chain–typically services.exe → svchost.exe–which serves as a proxy, making linking the behavior to the adversary's implant more difficult.
2. Services can be executed with SYSTEM privileges. This allows service execution to serve as a form of privilege escalation.
3. Under Windows 10 and 11, a significant portion of OS background operations has been migrated to services. Because there can be a lot of service activity on an endpoint, the analysis of services becomes more complex. This creates additional workloads for defenders to extract actionable information from potentially malicious services.

Organizations should look to centralize and build detections around standard Windows event logs related to creating new services to better detect anomalous service creation. Such logs are generated by default in the Windows Security event log using event id 4697 for a service creation and event id 7040 for modifications to the status of a particular service. Monitoring for services that reference files in anomalous locations, such as temp or user directories, or monitoring for services that execute popular LOLbins like powershell.exe, cmd.exe, rundll32.exe, or regsvr32.exe represent a low effort/high-value investment in the security of associated systems.

PowerShell: Still a Pivotal Tool in the Ransomware Affiliates' Playbook

PowerShell is a crucial component of many ransomware operators' execution TTPs, with the system administration tool being used in >65% of intrusions (see Figure 23 below).

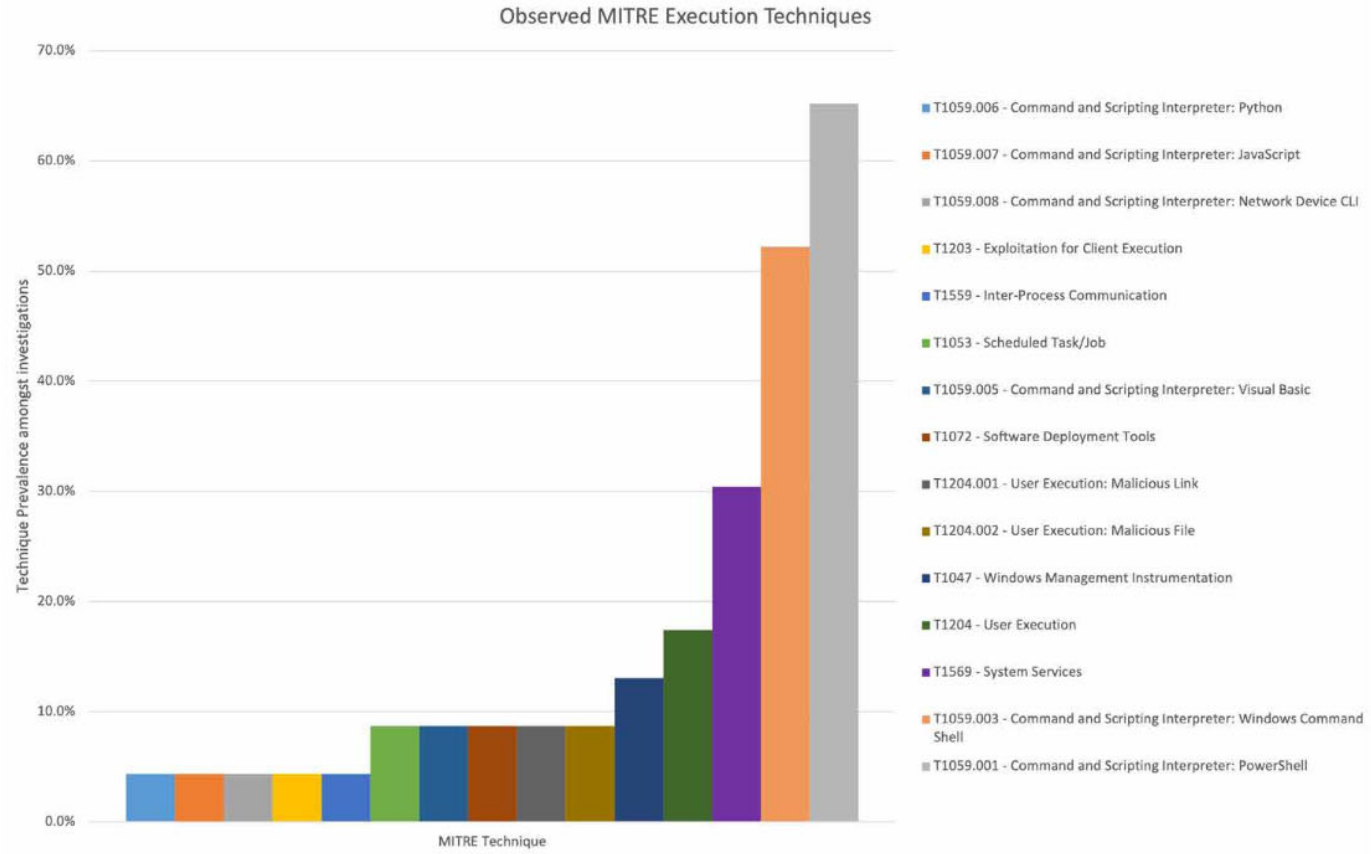

Figure 23 - MITRE execution techniques observed by the FortiGuard IR team throughout 2022.

While many organizations employ PowerShell for legitimate administration tasks–such as the separation of permissions across trusts, standardized scripts, and playbooks for administrative tasks involving PowerShell use–an increase in PowerShell logging makes it easier for organizations to identify and lock down anomalous usage.

Outside of these best practices, the best way for organizations to prevent adversaries from employing PowerShell in their environments is to deploy a modern EDR solution. Advanced EDR solutions (e.g., FortiEDR) allow defenders to baseline legitimate administrative command line activity in an environment (like PowerShell and cmd usage) and filter this routine activity so anomalous activity is automatically detected and blocked. While EDRs are not a silver bullet when defending a network, they are particularly effective at mitigating PowerShell deployed early in an intrusion before more complex EDR bypass techniques can be implemented.

Command and Control, Exfiltration, and Impact

Global Botnet Data

		Africa	Asia	Europe	N. America	Oceania	S. America
Command and Control	Application Layer Protocol	46%	46%	43%	57%	46%	54%
	Ingress Tool Transfer	33%	34%	25%	26%	18%	29%
	Uncommonly Used Port	21%	20%	32%	16%	35%	17%
	Commonly Used Port	0.04%	0%	0.09%	0%	0%	0%
	Non-Standard Port	0%	0%	0.010%	0.1%	0%	0%
Exfiltration	Automated Exfiltration	100%	100%	100%	0%	0%	0%
Impact	Data Encrypted for Impact	75%	94%	68%	94%	100%	98%
	Inhibit System Recovery	16%	5%	26%	6%	0%	0.4%
	Stored Data Manipulation	8%	0.4%	4%	0.3%	0.4%	2%
	Defacement	0.4%	0.2%	1%	0.2%	0%	0%
	Data Destruction	0.3%	0.1%	0.3%	0%	0%	0%

Figure 24 - Techniques in FortiSandbox Cloud data by tactic and region

It should come as no surprise that data encrypted for impact is the top tactic criminals use to close out their attacks across the board. With the growing prevalence of ransomware and wipers, encrypting data has become standard across all regions and industries. However, observed samples in our sandboxes also show an uptick in "Inhibit System Recovery" in Africa and Europe. This may be because of the growing practice of not paying ransom to regain control of systems, or it may just be a remnant of the samples we collected.

Botnets are nothing new in the cybersecurity world. They have been a part of the internet landscape since 2000 when Khan K Smith created one that sent 1.25 billion phishing emails through the EarthLink network. Twenty-three years later, malicious users worldwide are still finding ways to wreak havoc for personal gain using botnets.

Let's look at global botnet detections over the second half of 2022 and see what we can learn.

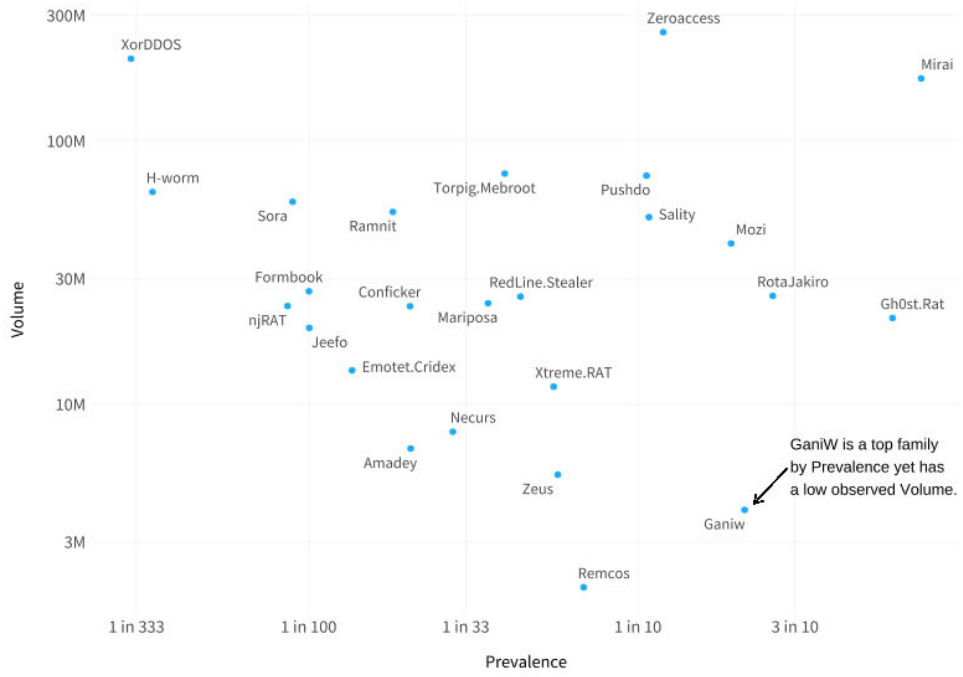

Figure 25 - Top 25 botnets by volume and by percent of organizations seeing them (prevalence)

First, let's look at botnets topping the charts in terms of both prevalence and volume. We see that many of the top botnet threats are older. In fact, out of the top five, only RotaJakiro seems to be from the 2020s. But while RotaJakiro was discovered in March 2021 targeting Linux64 systems, it had actually managed to maneuver undetected on systems going back to 2018 due to its ability to evade anti-malware. Researchers finally noticed something was awry when an ELF file of unknown purpose was discovered. That file had been communicating via four remote domains over HTTPS. Out of our data set, RotaJakiro impacted 25.7% of our sample. That's a far cry from the impact that Mirai and Gh0st Rat continue to have. Rounding out the top five are GaniW and Mozi. Mozi is currently considered to be one of the most active Mirai-style variants, according to IBM.

However, looking at the top ten by volume paints a different picture and introduces a few new names.

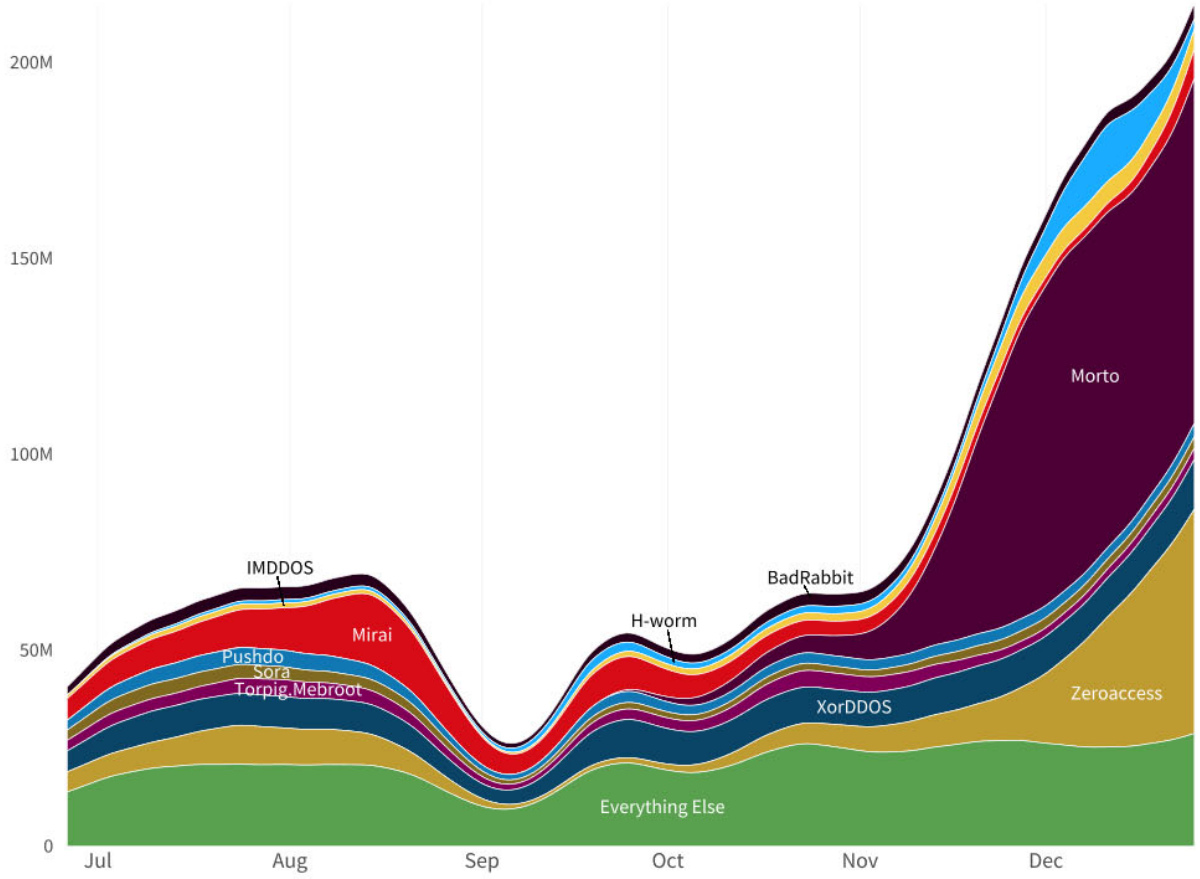

Figure 26 - Monthly volume of top 10 botnets

We see a stark incline starting in November 2022 for all botnet activity. 270.1 million hits were observed in November and 498.8 million in December. That's about an 85% increase in volume over just one month.

Morto accounted for a large portion of this dramatic increase, with 25.3 million hits in November and 84.6 million in December–more than a 3x increase. Morto was first observed in 2011. It was the first known worm to exploit Microsoft's Remote Desktop Protocol (RDP). Previous public research has shown that Morto doesn't necessarily target a specific vulnerability but heavily relies on users installing the worm on their system. It then uses brute force credential stuffing to gain access. However, the 12-year-old worm was not the only dramatic increase we documented over those 30 days. ZeroAccess activity also increased–from 26.3 million in November to almost 115 million in December–a more than 4x increase!

Initially discovered in 2011, ZeroAccess is a Peer-to-Peer (P2P) botnet that affects Microsoft operating systems. This botnet, like many others, initially makes its connections by prompting users to share a torrent file or engage with them in some way. Once that engagement happens, the malware turns the system into one of its many bots to continue on its path of bitcoin mining, information theft, or other activity the malicious user might be focused on. This botnet has traditionally been seen operating in bursts.

While it might be tempting to write off older threats as a thing of the past, it's increasingly clear that organizations must remain vigilant. Mirai wreaked havoc on the Internet when it first came on the scene in 2016. However, in early 2022, the botnet exploited CVE-2022-22965, also known as Spring4Shell. This critical remote execution vulnerability allowed malicious users to write into the webroot of a web server and then execute commands remotely. And even though a patch was quickly released, already compromised systems were letting their impact be felt, and the breadth of Mirai's impact continued to grow

Two new signatures were added to the FortiGuard encyclopedia during the second half of 2022:

1.https://www.fortiguard.com/encyclopedia/virus/10115376

2.https://www.fortiguard.com/encyclopedia/virus/10110647

Volume by Industry

Volume per Organization

short_name \ industry	Aerospace & Defense	Agriculture	Automotive	Banking/Finance/Insurance	Construction	Consulting	Education	Energy & Utilities	Environmental	Food & Beverage	Government	Healthcare	Legal	Manufacturing	Media/Communications	MSSP	Nonprofit	Retail/Hospitality	Technology	Telco/Carrier	Transportation and Logistics
Mirai	311	2.2k	727	479	169	1.4k	4.1k	277	208	162	848	336	174	5.7k	588	5.4k	428	747	2.4k	3.8k	328
Ramnit	590	358	70	365	140	40	2.4k	460	159	125	914	333	2	345	540	547	78	585	529	1.9k	288
Sality	263	259	1.8k	112	42	15	728	1k	15	56	332	1.4k	63	663	334	203	430	771	710	3.3k	287
Torpig.Mebroot	2.3k	200	284	177	202	56	2.4k	31	27	335	112	158	175	110	483	2k	44	155	713	2.6k	335
Sora		363	26	32	109	136	958	80	126	121	334	96		119	20	3.5k	4	802	329	3.9k	84
RedLine.Stealer	31	95	55	41	66	193	842	1.8k	122	58	303	169	16	142	183	558	170	72	221	3.4k	66
Morto			1.6k	534	6		108			356	2.7k	9		677	1	23k		1.1k	1.3k	133	82
Conficker	158	316	131	33	84	39	170	78	0.2	95	205	265	28	347	107	434	69	265	175	967	121
Formbook	61	23	11	56	167	89	193	419	42	32	84	62	8	388	82	567	8	331	268	1.5k	689
Zeroaccess	21	317	16	174	5	148	8.5k	23	9	4	515	16	2	72	144	3.2k	112	67	13k	11k	12
Gh0st.Rat	60	352	105	94	30	63	676	78	35	24	132	71	40	47	105	753	75	40	258	742	52
Mozi	12	20	9	295	42	198	1.3k	57	25	28	245	29	36	235	211	672	19	31	539	6.3k	11
BadRabbit		682		3k	936		0.2	2.5k		0.5	1.3k			4	1.1k	3.6k			579	661	
njRAT		85	0.2	4	36	26	550	50	34	159	429	408	7	375	367	259	3	114	223	2.1k	611
Emotet.Cridex	0	72	96	33	64	84	22	81	19	185	114	5	277	114	41	845	0.7	164	84	2.4k	317
Gozi	0.1	236	7	18	40	37	146	39	3	35	190	305	115	94	42	218	22	209	117	491	120
XorDDOS		1.3k	230	169	0	481	1.2k	0.1		224	1.6k	328	2.9k	9.1k	1.3k	40	0	0	3.1k	5.8k	39
H-worm	662	0.1	2	154		0	152	60		75	164	431	66k	51	330	586	0.1	17	147	489	529
RotaJakiro	13	948	5	21	3	17	2k	10	9	6	126	7	4	7	22	2.6k	117	97	162	1.3k	8
Necurs	8	83	69	11	13	12	106	82	3	136	124	81	0.3	26	85	35	90	108	145	411	3

top_threats/botnet_industry_volume

Figure 27

When we look at botnet activity by vertical, Morto has successfully targeted the Managed Security Service Provider (MSSP) industry with about 23,000 incidents. ZeroAccess, however, has set its sights on a few different sectors, including Education, Technology, and Telco/Carrier. And then you have Mirai now hitting OT, as you can see under the Manufacturing column in the chart above.

Volume by Region

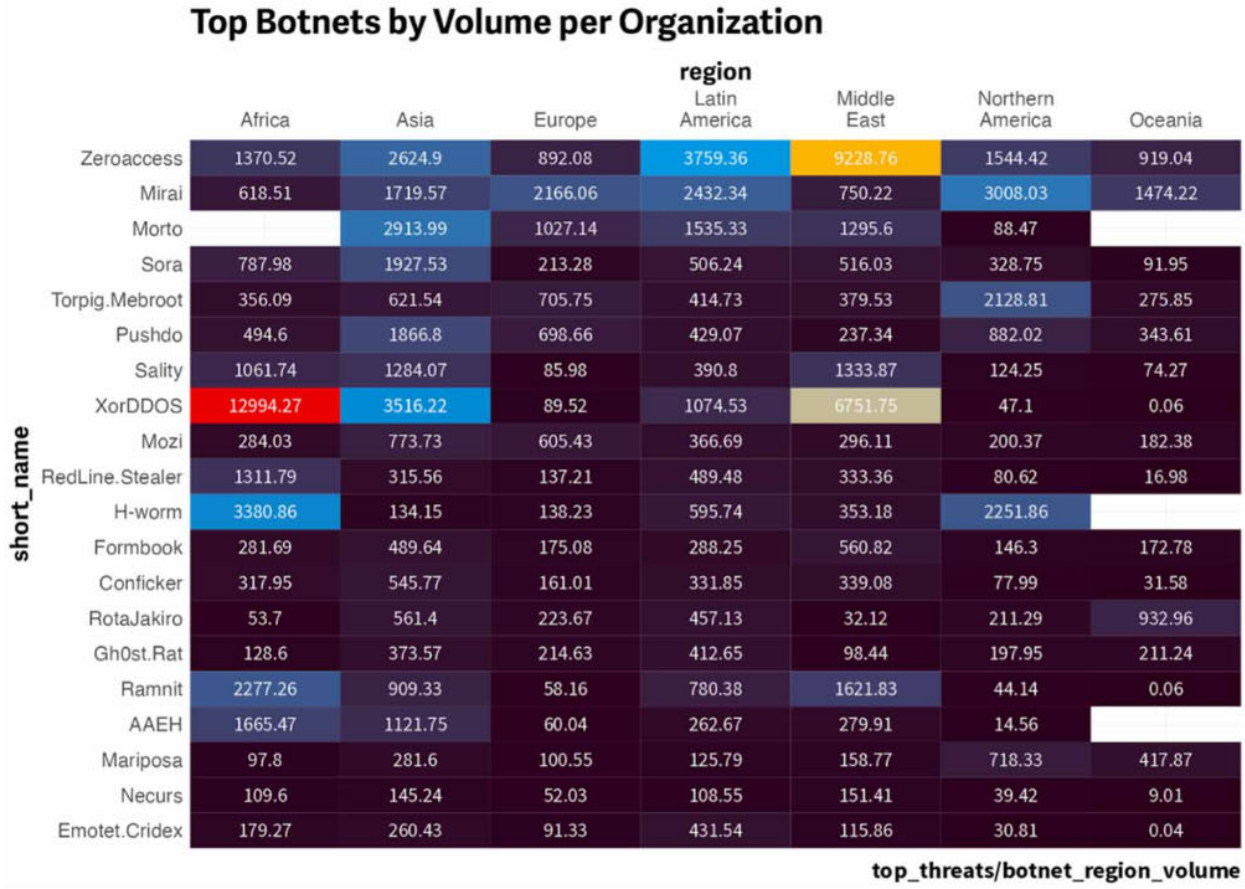

Figure 28

And when we look by region, we get an idea of where targeted endpoints were located. ZeroAccess seems to have impacted victims in the Middle East, Latin America, and Asia, while Morto appears to have targeted organizations in Asia. At the same time, XorDDoS heavily targeted endpoints in Africa. XorDDoS, first discovered in 2014, is a Linux Trojan malware kit known for its large DDoS campaigns and use of XOR encryption.

New Kids on the Bot

We've been talking a lot about older botnets that continue to dominate, but what about 2022's up-and-comers? While some are new, most are just "new-to-2022."

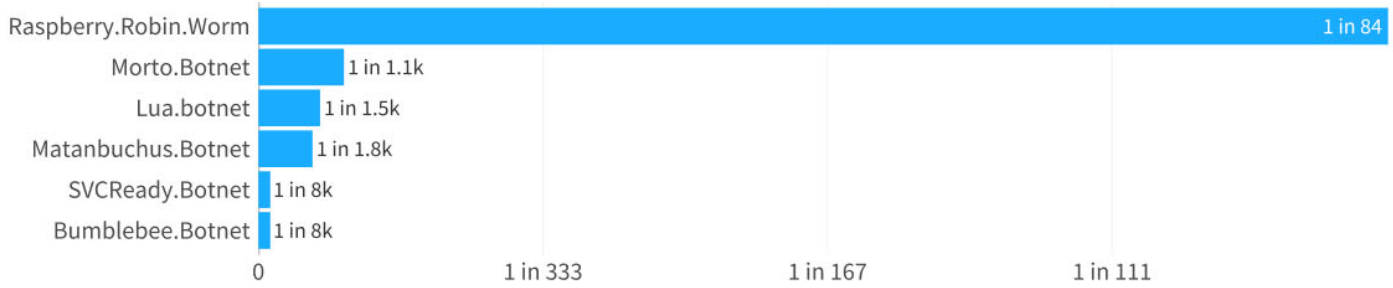

Figure 29 - Top five botnets unseen in the previous half, ranked by prevalence among organizations

When we look at the top signatures from the second half of 2022, one signature jumps out–RaspberryRobin. First spotted in September, RaspberryRobin primarily spreads in the government and telecommunications industries. Even though it's a new signature, it makes its way around using a tried and tested method–an infected USB stick (T1091 - Replication Through Removable Media). Once the USB is connected to a system, the worm can gain access. While there is no indication of what group might be responsible for RaspberryRobin, it has been linked to a SocGholish campaign from earlier in 2022.

In the second place, we can see that the Morto traffic discussed earlier in this section was not seen in the first half of 2022.

And in the third spot is Lua–a botnet discovered in 2016. It is the first Linux DDoS botnet coded entirely in (you guessed it) Lua, a programming language designed for applications.

Knowledge is Everything

Our Global Managed Detection and Response Team has observed an increase in blocks against RasberryRobin. It was so high that we needed to get a KB on how we protect against it.

Learn how EDR protects against RaspberryRobin malware.

Again, we're seeing a constant tug-of-war that places defenders between new threats and existing malware that may have fallen out of our collective security consciousness.

Insights from the Trenches

The FortiGuard Managed Detection and Response (MDR) team manages EDR instances on behalf of customers across the globe. Throughout their day-to-day activities, the MDR team works at the coalface of securing endpoints across thousands of global customers. This gives the team a significant snapshot of threat actor activities across business verticals and geopolitical regions. Similarly, our Intrusion Response (IR) team offers proactive and reactive services to support our global customer base. Exposure to customers actively fighting off a security incident provides valuable insight into intrusions initiated by APTs and financially motivated threat actors.

With a 200% growth (H2 over H1) of IR engagements, it's evident that organizations today feel more comfortable asking for external help. The insights below come from real-life cases observed by the FortiGuard MDR and IR teams throughout 2022. These insights provide practical recommendations on responding to both consistent and emerging features of the threat landscape and understanding how trends in the threat landscape shape customer impact and how customer actions shape these threats.

Exchange/OWA Exploitation Moves Beyond Initial Access and Becomes a Core Post-Exploitation TTP

While the exploitation of Microsoft Exchange servers for initial access was rampant in 2021 and early 2022 due to a swathe of critical remote code execution (RCE) vulnerabilities, post-exploitation activity targeting these servers has now become a mainstay for many threat actors' TTPs. The FortiGuard IR team has observed a trend in the latter half of 2022 where threat actors laterally moved to Exchange servers to establish persistence and perform collection activities in an already compromised environment.

In these situations, the threat actors either exploit external-facing services or engage access brokers to gain access to a network. But once these threat actors gain access, they perform internal reconnaissance and move to Exchange servers. And once they access the Exchange servers, they most commonly establish persistence through web shells (T1505.003 – Server Software Component: Web Shell). These web shells are then used for escalating privileges and accessing user credentials through OWA (Outlook on the web). This gives the adversary access to valid accounts, which are then used for lateral movement around a network through RDP, WMI (Windows Management Instrumentation), or SMB-based (Server Message Block) tools (e.g., PSEXEC).

We believe this widespread shift in post-exploitation TTPs results from years of abuse of Exchange, which has created threat actor familiarity and confidence in exploiting the platform. This familiarity and experience have given them visibility into platform features that can help them with a successful intrusion.

- Exchange servers are typically externally facing, with anomalous external connections expected as part of normal email operations. This makes an Exchange server a perfect place for web shells to hide among other activities.
- Exchange servers have large volumes of security events, resulting in rapid log turnover in most environments. This can hamper IR investigations in environments where logs are not centralized, or log retention policies do not support adequate data retention.
- Webpages that support OWA and other Exchange functions are not directly created by the IT team, and (blue team) knowledge of the Exchange backend is limited or not readily consumable.
- OWA may use a domain for authentication but may not include the same security features (i.e., no MFA).
- Emails typically include high-value personal information perfect for espionage (potential APT outcome) and extortion (potential FIN actor outcome)
- .NET accessibility through Exchange creates a great environment to deploy recently observed modular post-exploitation frameworks.

New malware (unknown signatures) is regularly employed post-exploitation within compromised Exchange servers, but the techniques used to support execution and persistence are not. Web shell deployment remains by far the most common execution/persistence technique on compromised Exchange servers. Payloads executed through web shells vary greatly but can still be detected by standard web shell exploitation behavioral indicators:

- Monitor for anomalous process spawns from the w3wp.exe process, especially cmd.exe and powershell.exe.
- Anomalous modification of typically static webpages (i.e., ashx, asp, and aspx) or creating webpages in usually static folders (webpages related to core Exchange operations are typically static).

Modules are predominantly reflectively loaded where web shells are used as part of larger, more complex toolsets (T1620 – Reflective Code Loading). This is likely done to subvert file-based signature detection (typical AV solutions) by avoiding writing payloads to disk. This also reduces the forensic evidence available to analysts and responders. But it also provides opportunities for modern toolsets like EDR products (e.g., FortiEDR) to shine as they catch these in-memory techniques.

BYO Malicious Bastion Host

The security posture of victim organizations continues to improve with the implementation of security controls and security endpoint software such as EDR. As a result, threat actors are finding alternative ways to maintain access and minimize detection.

One method to subvert these controls observed by the FortiGuard Incident Response team involves using a 'bastion host.' While this concept is not novel (T1612 – Build Image on Host), the technique is not widely observed. However, in the last half of 2022, our IR team investigated several instances where threat actors compromising a victim's hypervisor infrastructure installed their own VM. When a threat actor brings their own 'bastion host' in the form of a VM installed on their victim's infrastructure, they enjoy several benefits:

- It provides them with the freedom to maneuver within an environment. While many organizations have invested heavily in network visibility at the borders of their network, internal client-to-client network traffic remains a blind spot.
- Customers typically rely heavily on telemetry from endpoint security software installed on valid endpoints. However, a malicious bastion host does not have endpoint security software installed. If defenders are not checking for rogue endpoints, this creates a false sense of security.
- At the end of an operation, an adversary can remove the VM, which can significantly hamper IR and forensic activities and increase the longevity of adversary TTPs. Removing artifacts is particularly effective because the hypervisor uses shared hardware, making file retrieval from a deleted image extremely difficult.

This last technique is employed post-exploitation but may be difficult to detect if a hypervisor's management interface is internet-facing. In most cases, EDR solutions and AV products are not compatible with bare metal hypervisors (like ESXi). Because of this, if the adversary can exploit the management interface to gain access or can gain access by misusing legitimate credentials, victims may not detect the installation of a bastion host. To mitigate this, system owners should employ authentication schemes that prevent adversaries who have established a bastion host from authenticating with other network components.

In addition, defenders should monitor and maintain an up-to-date asset database to detect rogue endpoints in an environment. Alongside these checks, defenders should also ensure they have adequate IR playbooks to quickly respond to rogue endpoints and the likely compromise of their hypervisor infrastructure that supported its deployment.

Opportunistic Financial Crime Dominated the Limelight

Based on the assessed motivation behind incidents investigated by our IR team, opportunistic financially motivated crime resulted in the highest volume of incidents that required external support. See the Figure below for a graph of the assessed motivation.

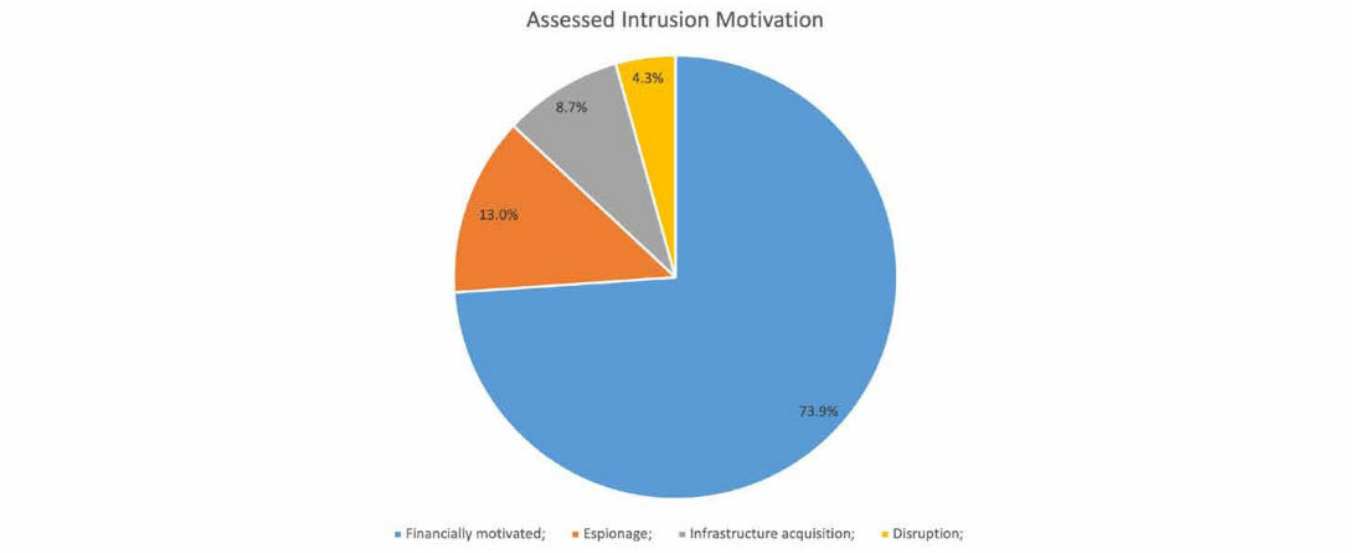

Figure 30 – Motivation for each intrusion the FortiGuard IR team observed in 2022.

Amongst financially motivated crime, ~82% of incidents involved the employment of ransomware or malicious scripts for T1486 – Data Encrypted for Impact. The ransomware landscape continues to evolve, with new families and variants being created daily as ransomware gangs form, break (or are broken by law enforcement operations), and reform. So it is essential to consider that, despite the names of the families and some of the technical aspects of the ransomware operation changing, many of the TTPs employed in an intrusion prior to the deployment of ransomware are the same between groups. This is partially attributed to the ransomware affiliate ecosystem, where affiliates deploy ransomware on behalf of various groups depending on their payout, and partly to the fact that victim networks still fail to mitigate ransomware operators' modus operandi.

Best Practices

- Gain network visibility and control by introducing network segmentation to reduce the impact and probability of spreading across your organization.
- Consistent security capabilities across the security surface–Anti-Botnet, DNS, URL, IPS, and AV–increase the chances of stopping an attack at one of its multiple stages.

Final Thoughts for the SOC Team

Understanding the most observed factors that contributed to an incident

It should be noted that the data in this section is biased because it is only taken from investigations conducted by the FortiGuard IR team. This means it only considers incidents where the victim was compromised to the point of requiring external support. It does not account for incidents effectively mitigated by customer controls nor incidents where the FortiGuard IR team was not engaged. Regardless of these biases, the data still provides valuable insight into what techniques contribute to large-scale intrusions.

Incidents investigated by our IR teams bridged multiple regions and spanned a broad range of industries, as shown in Figure 31 below.

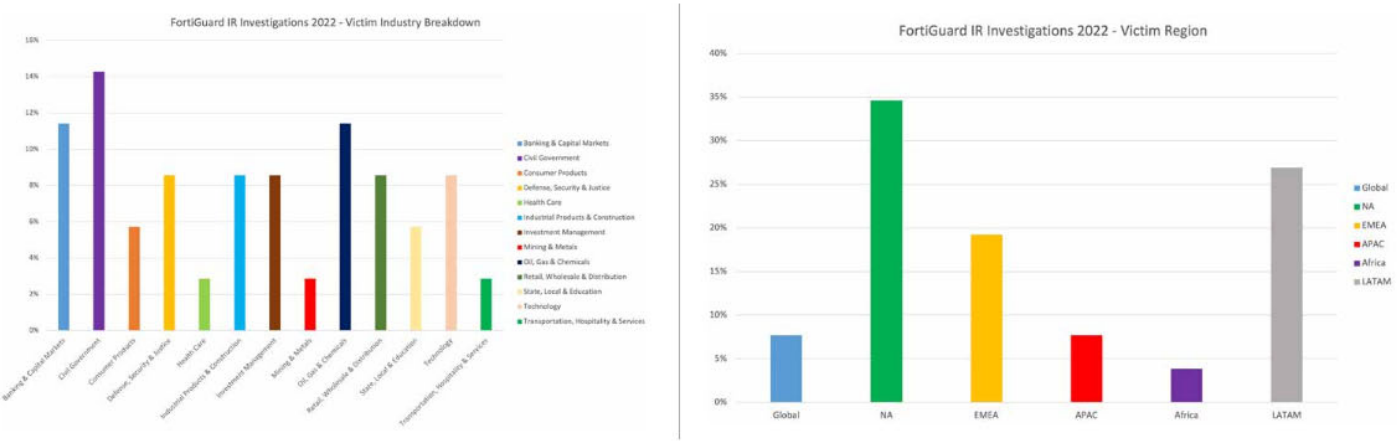

Figure 31 - Industry and region breakdown for victims investigated by the FortiGuard IR team in 2022

As part of our incident response process, we identify the factors that contributed to an organization's security incident so we can recommend where to focus efforts to prevent future intrusions. The collated outcome of these assessments is shown below, with contributing factors grouped.

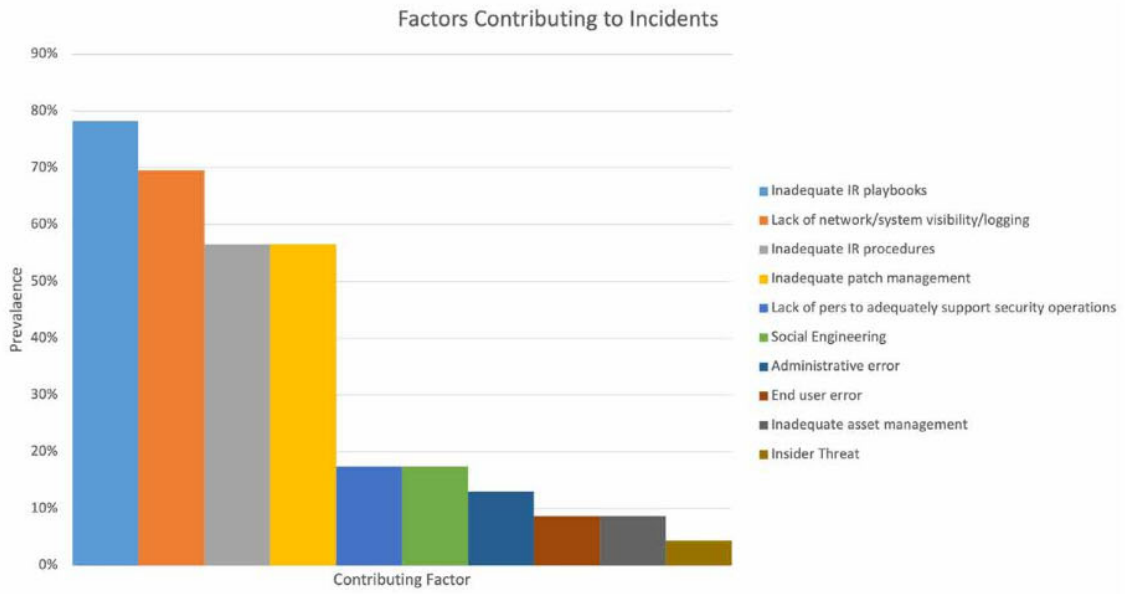

Figure 32 - Factors contributing to intrusions for incidents investigated by the FortiGuard IR team in 2022

As shown in this graph, the contributing factors that dominated incidents investigated by the FortiGuard IR team in 2022 included:

- **Inadequate IR playbooks (78%)** – The victim organization lacked the tactical playbooks to confidently detect or mitigate threats. In these cases, the customer had the tools to detect and mitigate but did not know how to effectively employ them to mitigate, contain, harden, or remediate threats associated with the intrusion.
- **Lack of network/system visibility/logging (70%)** – Victim organizations failed to detect initial indicators of compromise associated with the early stages of the kill chain. Data sources were not monitored, or the capabilities did not exist to detect them, preventing early mitigation and hampering an adequate response.
- **Inadequate IR procedures (57%)** – Victim organizations lacked direction for managing a security incident. This either resulted in a much longer time to respond or provided an inadequate response that allowed the adversary to still complete their mission (in many cases, the successful deployment of ransomware).
- **Inadequate patch management (57%)** – The victim organization failed to apply patches to known vulnerabilities within a reasonable timeframe. These vulnerabilities then became pivotal in an adversary progressing through their kill chain.

In most cases, fixing these deficiencies is primarily procedural. However, the issue of patch management continues to be a contributing factor to intrusions impacting organizations across the globe. In incidents we investigated, unpatched systems were typically known to victims, but they 'hadn't got around' to applying the required patches. In situations like this, it is highly recommended that critical patches be prioritized over other tasks assigned to the security team. A full-blown IR engagement caused by exploiting such vulnerabilities will alter existing priorities anyway, ensuring a more expensive pathway to applying the required patches.

The situation is similar where victims lack network and system visibility and/or logging. The victim had been stuck in a partial deployment of a security tool (such as an EDR), and a threat actor was able to compromise a network through an unprotected device. As with patching, the complete installation of security products and log centralization should be prioritized over other security functions. Incomplete implementations and gaps in visibility can create a false sense of security and inefficiencies in playbooks because there is a sense that something has been done. However, such inefficiencies make applying mitigations to ongoing intrusions difficult or impossible and give active adversaries freedom between defender actions to maintain access and increase the complexity of their investigations.

Organizations should regularly assess their network visibility to ensure they can detect intrusions at all stages of the adversary kill chain. To do this, organizations can look at the data sources available from their existing tools and then compare them to the data sources required to detect current threats to their environment. For example, there has been a recent spike in the use of OneNote macros for initial access. Organizations should ensure they can detect process creation events for common LOLbins processes from OneNote processes. If they can't, they should examine how to reconfigure existing security features to see these indicators.

When victim organizations lacked adequate IR procedures and playbooks, they struggled to respond effectively to an intrusion. This resulted in an extended engagement and a frustrated victim. Organizations should look to build and maintain a solid set of procedures and playbooks following industry best practices before an incident[1]. To support this, FortiGuard's IR team offers a number of proactive services that assist organizations in building Incident Response Plans (IRPs) and Incident Response Playbooks (IR Playbooks). Additionally, the team can assess existing IRPs and IR playbooks through an IR Readiness Assessment or interactive IR tabletop activities. In these activities, the FortiGuard IR team will work through scenarios with an organization's security teams and executives to 'battle test' their ability to respond effectively to various incidents.

Conclusion

Cybercriminals never let an opportunity go to waste. Whether it's a vulnerability, exploit, or international warfare, threats are always on the rise, especially when profit is to be made. Regularly monitoring and understanding new trends can help us proactively prepare for what's on the horizon, ensuring that our organizations stay up and running even in the event of an unexpected attack.

The past six months have also shown us that we cannot discount older threats–they are constantly evolving, looking for spaces that haven't been patched or new vulnerabilities that can help them proliferate. As an industry leader, we want you to feel confident in protecting your business. We do that by providing you with a comprehensive view of how the threat landscape is evolving from a high-level perspective and highlighting critical tools you can implement to improve your cybersecurity posture, ensuring you don't leave any gaps in your protections.

Most importantly, our experts are always here to help. We look forward to updating you again on the evolving threat landscape in our next report!

You Have the Opportunity to Protect and Mitigate

So now that you have gained critical insights into what has happened over the last six months, the question remains: "What can you do about this wide variety of threats, the growing volume of malware variants, and evolving and sophisticated ATPs?

One of the most important steps is to ensure that the products you rely on to address these challenges can leverage artificial intelligence (AI), machine learning (ML), and deep learning (DL), along with other advanced analytics. These capabilities enable your solutions to:

- Keep up with processing the enormous volume of event data generated by today's digital organizations.
- Identify anomalous and high-risk activity that often mimics legitimate operations anywhere across your distributed network.
- See your entire attack surface and cyber kill chain stages to establish comprehensive visibility even as your network evolves.
- Integrate with traditional security controls within a cybersecurity platform to simplify and speed operations, ensure consistent policy enforcement, and automate a unified response to threats.

If you're concerned about understanding your increasingly complex environment or are facing challenges created by the cybersecurity skills gap, consider engaging MDR (Managed Detection and Response) experts for your EDR instances. These security experts can seamlessly augment your team to regularly tune your defenses, understand where your legitimate business applications are being used maliciously, threat hunt your environment for emerging threats and help you keep your eye on alerts while providing 24×7 remediation. Learn more about MDR.

Threat Landscape Report Glossary: Fortinet Tools

MITRE ATT@CK STAGES	WHAT THE BAD GUYS DO	WHAT WE SHOULD DO
Reconnaissance, Resource Development	The adversary is 1. Trying to gather information they can use to plan future operations 2. Trying to establish resources they can use to support operations.	FortiDeceptor provides a non-intrusive, agentless OT/IT/IoT deception solution to detect active in-network threats. Decoys generate high-fidelity, actionable alerts resulting in an automated incident response to help stop zero-day attacks. The solution flags early-stage active, in-network reconnaissance that precedes actual cyberattacks. It also detects ransomware, stolen credential usage, privilege escalation, lateral movement, data collection, port and server scanning, and other threat activities. The FortiRecon service scans the internet, dark web, open-source, and underground and open forums to automatically discover known/unknown internet-facing assets, vulnerabilities, and misconfigurations. It detects leaked credentials and data, as well as continuously monitors and alerts on changes made to an organization's digital footprint across the web, social channels, and app stores. Leveraging industry-leading AI-enabled security with FortiGuard threat research team expertise, the service alerts on brand infringements and offers key insights and guidance on remediation prioritization. It also executes takedowns of phishing sites, rogue mobile apps, fake social media accounts, typo squatting, and more to help you continuously enhance your security posture, and protect your brand and customers from cyber threats.
Initial Access	The adversary is trying to get into your network. Initial access consists of techniques that use various entry vectors to gain an initial foothold within a network. Techniques used to gain a foothold include targeted spearphishing and exploiting weaknesses on public-facing web servers.	Inline Sandbox solutions include multiple ML engines to provide static analysis of code in transit and the dynamic analysis of code running in a secure, instrumented environment. Further, FortiNDR's Virtual Security Analyst utilizes an artificial neural network to provide sub-second detection of previously unknown malware, including insight into its feature makeup, comparing it against more than two dozen common threat classes. Both products can be integrated across multiple attack vectors to identify code seeking entry via email, the web, various cloud applications, and more and then automate corresponding response actions.
Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, and Collection		FortiEDR identifies vulnerable applications and shields them from exploit while an ML engine blocks the installation of malicious code without the need for pre-existing threat intelligence. Behavior analytics, both on the device (for patented detect and defuse of running code) and a dynamic control flow engine in the cloud continue classifying and reclassifying system activity. A predefined response framework automates the containment and remediation function. FortiGuard IPS provides near-real-time intelligence with thousands of intrusion prevention rules to detect and block known and zero-day threats before they reach your devices. The service is augmented by our in-house research team, credited with more than 1,000 zero-day detections. SOC augmentation tools like SOCaaS and FortiAnalyzer, including IOC and Outrbreak Detection Services, are part of the Fortinet Security Fabric. FortiAnalyzer provides security fabric analytics and automation to provide better detection and response against cyber risks

MITRE ATT@CK STAGES	WHAT THE BAD GUYS DO	WHAT WE SHOULD DO
Command and Control, Exfiltration, and Impact		FortiNDR utilizes an ML engine to profile network activity and identify deviations (including new outbound communications) along with a series of pragmatic analytics to identify additional indicators of risk, such as weak ciphers, vulnerable protocols, and IoCs related to ongoing cybercampaigns. Integrations with the firewall, security orchestration, playbooks, automation, and response platforms speed investigation and containment. Many of these products can identify the action on objectives (Impact) of cybercriminals, including compromised devices, lateral movement, data exfiltration, data encryption, and more. The FortiGate Next-Gen Firewall, with FortiGuard AI-Powered Security Services natively integrated includes: ■ Web Security ■ Device Security ■ Content Security
Continuously Assess and Improve		■ FortiTester for Performance and Breach Attack Simulation ■ Assessments Readiness services for continuous cycle of evaluation and calibration of your risk posture. ■ Security Awareness & Training to create a cyber-aware workforce. ■ FortiSOAR integrated into the Fortinet Security Fabric provides security orchestration, automation, and response (SOAR) for innovative case management, automation, and orchestration.

[1] https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

FORTINET

www.fortinet.com

February 21, 2023 11:11 PM

1471550-0-0-EN